



FACULTAD DE DERECHO

CRIPTOMONEDAS Y BLANQUEO DE CAPITAL: UN ANÁLISIS PENAL Y REGULATORIO DE UN DESAFÍO ESTRUCTURAL

Autor: Claudia Cobo Gémar

5º E-3 A

Área de Derecho Penal

Tutor: Borja Almodóvar Puig

Madrid

Junio 2025

ÍNDICE

1. INTRODUCCIÓN.....	5
2. MARCO TEÓRICO	5
2.1. Definición y concepto criptomonedas	5
2.1.1. Contexto y dificultades de definición.....	5
2.1.2. Criptomoneda: concepto, naturaleza y distinción	6
2.2. Las criptomonedas frente al dinero en sentido jurídico	8
2.2.1. Funcionamiento de la tecnología blockchain.....	9
2.2.2. Características jurídico-relevantes de la tecnología blockchain	10
2.3. El ecosistema de las criptomonedas: usuarios, transacciones, wallets y exchanges	13
2.3.1. Monederos digitales (wallets).....	14
2.3.2. Exchanges.....	15
2.4. La aproximación jurídica a las criptomonedas: retos conceptuales y normativos....	16
2.3.3. Las criptomonedas como bienes en el Derecho español.....	17
3. REGULACIÓN DEL BLANQUEO DE CAPITALS	18
3.1. Concepto.....	18
3.2. Evolución y fundamentos normativos	19
3.3. Naturaleza penal del blanqueo de capitales: el artículo 301 del Código Penal.....	20
3.3.1. Bien jurídico protegido.....	20
3.3.2. Elementos del tipo	21
3.3.3. Fases tradicionales del blanqueo y su ejecución con criptoactivos.....	30
3.4. Regulación administrativa	31
3.4.1. Normativa europea:	31
a. Los mecanismos de prevención en la regulación europea: principales medidas ...	33
3.4.2. el Reglamento MICA.....	35
a. Objetivos del reglamento MICA	36
b. Proveedores de servicios sobre criptoactivos (CASps)	36
c. Obligaciones relevantes de MiCA en relación con la prevención del blanqueo de capitales.....	37
d. Crítica doctrinal sobre los límites del ámbito de aplicación del Reglamento MiCA	38
3.4.3. El reglamento AML: consolidación del marco preventivo y apoyo estructural a la persecución penal del blanqueo con criptoactivos	39
a. Naturaleza y finalidad del Reglamento AML.....	39
b. Aportaciones relevantes para la prevención y detección penal	39

c.	Valoración crítica y límites del instrumento	40
3.4.4.	Normativa española: la Ley 10/2010	41
4.	CARACTERÍSTICAS ESTRUCTURALES DE LOS CRIPTOACTIVOS QUE FAVORECEN SU USO COMO INSTRUMENTO DE BLANQUEO DE CAPITALES.....	41
4.1.	Descentralización y desintermediación: la exclusión del control institucional	41
4.2.	La desintermediación y sus implicaciones para la prevención y detección	42
4.3.	Posibilidades de segmentación, diseminación y reconversión del capital	43
4.4.	Comparación con el dinero en efectivo: ¿mayor o menor peligrosidad?	44
4.5.	Riesgos añadidos por el carácter irreversible y la dificultad de reacción estatal.....	44
4.6.	Conclusión: una herramienta de riesgo estructural	45
5.	PROPUESTA DE LEGE FERENDA: ¿ES NECESARIO MODIFICAR O REFORZAR EL ACTUAL ART. 301 CP PARA SANCIONAR NUEVAS CONDUCTAS DE BLANQUEO?	45
5.1.	Adecuación y límites del artículo 301 frente al Uso de Criptoactivos	45
5.2.	Capacidad del tipo penal para abordar las técnicas modernas de blanqueo.....	46
5.3.	La insuficiencia parcial del marco administrativo-preventivo	47
5.4.	¿Reformar el tipo penal? Argumentos para una respuesta negativa.....	48
6.	RESUMEN DE CONCLUSIONES	49
7.	BIBLIOGRAFÍA.....	51
1)	LEGISLACIÓN	51
2)	JURISPRUDENCIA.....	51
3)	OBRAS DOCTRINALES	52
4)	RECURSOS DE INTERNET	53

RESUMEN EJECUTIVO

El presente Trabajo de Fin de Grado analiza el delito de blanqueo de capitales desde una doble perspectiva: su tipificación penal en el ordenamiento jurídico español y su adaptación ante el uso creciente de criptomonedas y tecnología blockchain como medios de comisión. El estudio parte de un enfoque teórico riguroso basado en doctrina, jurisprudencia y normativa europea e internacional, y culmina con un análisis crítico sobre los retos que plantea la trazabilidad jurídica de las operaciones con criptoactivos frente a su aparente trazabilidad técnica.

Se identifican tres niveles de análisis: la configuración típica del delito en el Código Penal, las obligaciones de diligencia en el plano administrativo, y el impacto de las características técnicas del sistema blockchain (pseudonimato, descentralización e inmutabilidad). El trabajo sostiene que las criptomonedas no exigen una reforma del tipo penal, pero sí una mayor adaptación normativa para imputar por imprudencia a personas jurídicas en el contexto digital.

El TFG concluye que la trazabilidad técnica que permite la blockchain no se traduce en una trazabilidad jurídica eficaz, lo que genera un desafío específico en la prevención y persecución del blanqueo de capitales.

Palabras clave: blanqueo de capitales, criptomonedas, blockchain, responsabilidad penal, trazabilidad, personas jurídicas, normativa europea.

ABSTRACT

This project analyzes the crime of money laundering from a dual perspective: its criminal classification under Spanish law and its adaptation to the growing use of cryptocurrencies and blockchain technology as a means of committing it. The study is grounded in rigorous legal theory, jurisprudence, and European and international regulations, and concludes with a critical reflection on the legal traceability challenges posed by crypto-assets, despite their apparent technical traceability.

Three levels of analysis are considered: the legal configuration of the offense in the Spanish Penal Code, due diligence obligations in administrative law, and the legal impact of blockchain features (pseudonymity, decentralization, immutability). The paper argues that cryptocurrencies do not require a reform of the criminal definition, but they do demand greater regulatory adaptation to allow criminal liability for negligence, especially in legal persons.

The study concludes that blockchain's technical traceability does not entail effective legal traceability, which constitutes a critical challenge in combating money laundering.

Keywords: money laundering, cryptocurrencies, blockchain, criminal liability, traceability, legal persons, European regulation.

1. INTRODUCCIÓN

El fenómeno de los criptoactivos ha supuesto una transformación radical en las formas de gestionar, transferir y almacenar valor económico en el ámbito digital. Desde su irrupción con el nacimiento de Bitcoin, estas tecnologías han desafiado no solo los marcos financieros tradicionales, sino también los sistemas jurídicos encargados de regular y controlar su uso. Entre las múltiples implicaciones que plantea esta revolución tecnológica, una de las más relevantes y controvertidas es su potencial utilización como instrumento para el blanqueo de capitales.

El presente trabajo se propone analizar, desde una perspectiva jurídico-penal y preventiva, el impacto que el uso de criptoactivos tiene en el delito de blanqueo de capitales regulado en el artículo 301 del Código Penal. El objetivo principal es determinar si esta nueva realidad exige una modificación del tipo penal o si, por el contrario, el marco normativo actual es suficiente para sancionar dichas conductas.

Para ello, el estudio se estructura en tres bloques complementarios. En primer lugar, se realiza una aproximación técnica y conceptual al ecosistema cripto y a las características que lo diferencian de los sistemas tradicionales, poniendo énfasis en aquellos elementos que pueden dificultar la trazabilidad y facilitar el anonimato. En segundo lugar, se examina el marco normativo vigente, tanto en su vertiente penal como administrativa, evaluando las capacidades y límites del artículo 301 CP frente a las técnicas modernas de blanqueo y la respuesta ofrecida por normas como la Ley 10/2010, el Reglamento MiCA y las directivas AML. Finalmente, se plantea una reflexión crítica en clave de *lege ferenda*, para valorar si el tipo penal requiere ser reformulado o si la solución pasa por fortalecer la cooperación institucional, la interpretación jurisprudencial y el marco administrativo preventivo.

Este trabajo no parte de certezas cerradas, sino de una preocupación real por comprender si la actual configuración normativa resulta suficiente ante un fenómeno tecnológico complejo y cambiante. Solo a través de un análisis jurídico riguroso que combine perspectivas dogmáticas, técnico-operativas y preventivas podrá determinarse si el marco actual exige ajustes, o si los desafíos planteados por los criptoactivos pueden afrontarse desde el interior de las categorías y mecanismos ya disponibles.

2. MARCO TEÓRICO

2.1. Definición y concepto criptomonedas

2.1.1. Contexto y dificultades de definición

Hasta fechas recientes, la ausencia de una “gramática” jurídica y técnica común sobre las criptomonedas ha constituido uno de los principales obstáculos para su adecuada definición y conceptualización¹. Bajo el amplio paraguas de “Moneda virtual” se han englobado realidades diversas y heterogéneas, como los tokens, los activos virtuales o las

¹ Sanz Bayón, P., “Análisis sobre la naturaleza jurídica de las criptomonedas y la regulación europea de los proveedores de servicios de cambio y de custodia de monederos electrónicos”, *Revista de Derecho Bancario y Bursátil*, Nº 160, 2020, pp. 69-110

propias criptomonedas, dificultando su encuadre en un marco conceptual unívoco. En este contexto, comprender qué es una criptomoneda exige, en buena medida, delimitar con precisión todo aquello que no es.

La entrada en vigor del Reglamento (UE) 2023/1114, relativo a los mercados de criptoactivos (MiCA) ha supuesto un avance significativo hacia la clarificación terminológica en el ámbito europeo, al introducir definiciones normativas como la de criptoactivo, token referenciado a activos o token de dinero electrónico². No obstante, la armonización conceptual todavía enfrenta retos, especialmente en el plano doctrinal y en su aplicación a fenómenos emergentes como las finanzas descentralizadas (DeFi) o las *stablecoins* algorítmicas.³

Es habitual, tanto en el lenguaje jurídico como en el divulgativo, encontrar referencias indistintas a términos como “criptomoneda”, “criptoactivo”, “moneda virtual” o “criptodivisa”, a pesar de referirse en ocasiones a realidades técnicas y funcionales distintas. En la doctrina especializada se ha advertido que esta falta de precisión conceptual genera confusión y dificulta tanto la aplicación normativa como la detección de riesgos jurídicos asociados.⁴

2.1.2. Criptomoneda: concepto, naturaleza y distinción

En términos generales, puede entenderse por criptomoneda “una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda de curso legal, que no tiene la consideración de moneda o divisa, pero es aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos”⁵. Otros autores subrayan que estas unidades pueden utilizarse tanto como medio de intercambio como reserva de valor, permitiendo cierta independencia del sistema financiero tradicional.⁶

En este contexto, conviene diferenciar las criptomonedas de otras categorías afines. Así, resulta pertinente delimitar los conceptos de *moneda virtual*, *token* y *criptoactivo*, con el objetivo de evitar equívocos conceptuales que puedan dificultar su análisis jurídico. No existe en la doctrina un criterio unívoco respecto a la clasificación de estos activos: algunos autores consideran que la criptomoneda constituye una subcategoría de las monedas virtuales, mientras que otros entienden que se trata de figuras autónomas, tanto desde el punto de vista técnico como funcional.⁷

² Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA), y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937.

³ Rodríguez Quejido, V. (2019). *Criptoactivos: naturaleza, regulación y perspectivas* (Documento de trabajo ODF n.º 29). Instituto de Estudios Fiscales. https://www.ief.es/docs/destacados/DT_29.pdf

⁴ Véase, por ejemplo: Chamorro Rodríguez, M.ª de la C. (2019). *Aspectos jurídicos de las criptomonedas*. Blockchain Intelligence. <https://www.blockchainintelligence.es>. Doménech Ariza, P. M. (2023). *Blanqueo de capitales y financiación del terrorismo mediante el uso de criptodivisas. Nuevas regulaciones* [Trabajo fin de grado, Universidad Internacional de La Rioja].

⁵ Uría Menéndez. (2018). *Monedas virtuales: Aproximación jurídico-tributaria y control tributario*. Actualidad Jurídica Uría Menéndez, (48), 72-81

⁶ Mancini, G. (2020). *Criptoactivos y blanqueo de capitales*. Revista Española de Derecho Financiero, (187), 33-57.

⁷ Chamorro Rodríguez, M.ª de la C. *Op. Cit.*, n.

En todo caso parece razonable entender que las monedas virtuales comprenden toda representación digital de valor no emitida ni garantizada por una autoridad pública, que no posee estatuto jurídico de moneda o dinero, pero que puede utilizarse como medio de intercambio por personas físicas o jurídicas en determinados contextos, ya sean abiertos o cerrados, y que puede transferirse, almacenarse o negociarse electrónicamente.⁸

Las criptomonedas, en cambio, se caracterizan por ser sistemas de intercambio descentralizados, que operan sobre redes basadas en tecnología blockchain, utilizando técnicas criptográficas avanzadas para validar y asegurar las transacciones sin necesidad de intermediarios financieros o institucionales. Ejemplos de ellas serían el bitcoin, ether, litecoin o dogecoin⁹. A diferencia de otras monedas virtuales, no dependen de una autoridad emisora centralizada, sino que su emisión y validación se rigen por protocolos abiertos, en los que intervienen nodos distribuidos y mecanismos de consenso como el *Proof of Work* o el *Proof of Stake*¹⁰. Estas estructuras garantizan la inmutabilidad del registro y permiten una trazabilidad pseudónima, lo que a su vez plantea importantes desafíos jurídicos. Esta concepción técnica permite diferenciarlas con claridad del resto de monedas virtuales y responde a la formulación original de Satoshi Nakamoto, quien en 2008 definió Bitcoin como un sistema de dinero electrónico *peer-to-peer* que permite pagos directos entre usuarios sin necesidad de intermediarios financieros.¹¹

Por su parte, los tokens representan unidades digitales emitidas generalmente por plataformas blockchain que pueden representar una amplia variedad de derechos de uso, acceso, participación o de contenido económico—. No necesariamente cumplen funciones monetarias,¹² por lo que no deben confundirse con las criptomonedas, aunque compartan el mismo soporte tecnológico. Según su diseño, pueden otorgar acceso a servicios o plataformas digitales, representar derechos económicos o de participación (como en los security tokens), servir como herramienta de gobernanza dentro de protocolos descentralizados o simbolizar activos únicos no intercambiables, como sucede con los non-fungible tokens (NFTs). En este sentido, los tokens pueden representar derechos de uso, acceso, contenido o valor económico, pero no necesariamente cumplen funciones monetarias como las criptomonedas, aunque compartan con ellas la infraestructura tecnológica basada en blockchain. Por ello, su tratamiento jurídico exige una diferenciación funcional clara, en función del tipo de token y del ecosistema en el que opera.

Esta ambigüedad se traslada también al plano normativo. La Directiva (UE) 2018/843 se refiere a las monedas virtuales con una definición funcional, definiéndolas como representaciones digitales de valor aceptadas como medio de intercambio, pero no emitidas ni garantizadas por una autoridad pública. Mientras que el Reglamento (UE)

⁸ Parlamento Europeo y Consejo. (2018). *Directiva (UE) 2018/843*, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849. Diario Oficial de la Unión Europea

⁹ Barrio Andrés, M. (2022). La nueva regulación de los criptoactivos en España. Diario La Ley, (10010).

¹⁰ Ibáñez Jiménez, J. W. *Derecho de Blockchain y de la tecnología de registros distribuidos*, Aranzadi, 2018, p.21. y LEGERÉN-MOLINA, A., “Retos jurídicos que plantea la tecnología de la cadena de bloques (Aspectos legales de blockchain)”, Revista de Derecho Civil, Vol. 6, N.º 1, 2019, pp. 177-237.

¹¹ El modelo descentralizado *Peer-to-Peer* en el que se basa Bitcoin fue formulado por su creador bajo pseudónimo en el documento técnico que presentó públicamente en 2008. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>

¹² Chamorro Rodríguez, M.ª de la C. *Op. Cit.*,

2023/1114 (MiCA) opta por el concepto más amplio de *criptoactivo*, incluyendo bajo esta categoría tanto a las criptomonedas como a otros activos digitales con funciones diversas¹³. Por tanto, no todos los criptoactivos son criptomonedas, ni todas las criptomonedas pueden calificarse como monedas en sentido jurídico.

2.2. Las criptomonedas frente al dinero en sentido jurídico

Para finalizar con la conceptualización, conviene advertir que las criptomonedas no pueden considerarse dinero en sentido jurídico estricto, ya que carecen de los tres atributos esenciales que caracterizan al dinero tradicional: unidad de cuenta, medio de pago y depósito de valor reconocido legalmente.¹⁴ Según la normativa europea, el dinero electrónico debe estar respaldado por una entidad regulada y cumplir con requisitos de convertibilidad con moneda fiduciaria, condiciones que muchas criptomonedas no satisfacen, lo que impide su reconocimiento oficial como dinero.¹⁵ Aunque la polémica doctrinal sobre su posible equiparación al dinero no está del todo resuelta, sí puede afirmarse que únicamente puede considerarse medio de pago legal aquel reconocido como tal por el Estado. No obstante, ello no impide que las criptomonedas puedan ser utilizadas como medio de pago contractual en relaciones privadas¹⁶, en virtud del principio de autonomía de la voluntad.¹⁷ De hecho, su propia concepción técnica y filosófica —ya anticipada por Wei Dai en 1998 al proponer un sistema de dinero descentralizado basado en criptografía— revela una voluntad deliberada de crear una alternativa al dinero tradicional,¹⁸ prescindiendo de emisores centralizados y autoridades de control.

En definitiva, en el presente trabajo se utilizará el término *criptomonedas* para referirse a aquellos criptoactivos diseñados como medio de intercambio, basados en tecnología blockchain, descentralizados y no respaldados por autoridad pública alguna. Aunque el concepto de criptoactivo engloba categorías más amplias, como los tokens referenciados a activos o de utilidad, este estudio se centrará en las criptomonedas con vocación de circular como dinero alternativo, por ser las que presentan mayor relevancia en el análisis penal del blanqueo de capitales.

¹³ Parlamento Europeo y Consejo. (2023). *Reglamento (UE) 2023/1114*, relativo a los mercados de criptoactivos. Diario Oficial de la Unión Europea.

¹⁴ Chamorro Rodríguez, M.^a de la C. *Op. Cit.*

¹⁵ Suárez Puga, E. A. (2020). *Naturaleza y régimen jurídico de las criptomonedas*. Universitat Pompeu Fabra y ESADE Law School. Recuperado de <https://www.pensamientopenal.com.ar/system/files/2021/08/doctrina89427.pdf> [consulta: 24 de marzo de 2025].

¹⁶ Ibáñez Jiménez, Legerén-Molina *Op. Cit.*, n.

¹⁷ Código Civil español, art. 1255

¹⁸ Dai, W. (1998). *b-money*. Recuperado de <http://www.weidai.com/bmoney.txt> [consulta: 24 de marzo de 2025].

2.2.1. Funcionamiento de la tecnología blockchain

La tecnología blockchain, o cadena de bloques, es un tipo de tecnología de registro distribuido (DLT) ¹⁹ que funciona como una base de datos digital compartida. En ella, se registran transacciones de manera secuencial, verificable y descentralizada, sin necesidad de una autoridad central o intermediario,²⁰ ya que, son los propios participantes de la red quienes verifican y validan cada operación.

Cada transacción en la blockchain se registra de forma cronológica y permanente, igual que en un libro mayor contable tradicional. Sin embargo, a diferencia de un sistema centralizado, este registro se encuentra replicado en múltiples nodos —ordenadores conectados a la red—, que verifican y actualizan simultáneamente la información. Esta validación colectiva sigue un protocolo común, lo que garantiza la integridad y transparencia del sistema²¹. Cada operación se agrupa junto a otras en estructuras denominadas bloques, que contienen un número determinado de transacciones, un sello temporal y una huella criptográfica (hash) del bloque anterior, lo que asegura su conexión con el resto de la cadena.²²

Su funcionamiento se basa en una red de nodos distribuidos, cada uno de los cuales conserva una copia actualizada y sincronizada de toda la cadena. Para incorporar un nuevo bloque, este debe ser validado por la mayoría de los nodos mediante mecanismos de consenso, como el Proof of Work (PoW) ²³o el Proof of Stake (PoS). Estos sistemas sustituyen la figura del intermediario por un proceso colectivo de verificación. Como ningún nodo tiene autoridad exclusiva sobre la cadena, cualquier intento de alteración es detectado por el resto, lo que garantiza la seguridad y consistencia del sistema.

Una vez que un bloque ha sido validado e incorporado a la cadena, su contenido ya no puede modificarse sin alterar todos los bloques siguientes. Esta característica técnica proporciona al sistema una inmutabilidad práctica, es decir, una resistencia efectiva frente a cualquier intento de manipulación. Por ello, la doctrina ha descrito la blockchain como

¹⁹ Según la forma en que se comunican los nodos (ordenadores) que conforman la red de un sistema, pueden encontrarse tres tipos de redes: centralizadas, descentralizadas y distribuidas. En las redes centralizadas, un único nodo controla y gestiona toda la información, lo que las hace vulnerables si dicho nodo falla o es comprometido. En las descentralizadas, los nodos operan sin un control central estricto, aunque puede haber ciertos grupos que concentren parte de la comunicación. Por su parte, en las redes distribuidas —como las que emplea la tecnología blockchain—, todos los nodos se conectan directamente entre sí, sin jerarquías, lo que impide que uno solo pueda alterar el sistema y garantiza mayor seguridad, resistencia y transparencia. González, A. (2021). *Blockchain como inicio de la revolución tecnológica del sector financiero*. En J. M. Corchado y J. L. Tejedor (Eds.), *C1b3rWall Academy - Módulo 0*. Universidad de Salamanca.- [está bien citado o hay que poner la cita entre paréntesis?]

²⁰ Los ordenadores o nodos pueden comunicarse sin necesidad de un servidor central que lo facilite. Preukschat, A., “Blockchain: la revolución industrial de internet”, *Gestión 2000*, 2017, pp.23-24.

²¹ Martínez Boada, J., & Rejas Muslera, R. (2024). *Protección jurídica de Blockchain: Un análisis desde su funcionalidad y naturaleza jurídica según el ordenamiento jurídico español*. *Revista Chilena de Derecho y Tecnología*, 13, e73869. <https://doi.org/10.5354/0719-2584.2024.73869>

²² León Bazan, Y. Y., & Delgado Guerrero, J. S. (2024). *Contratos inteligentes a partir de una especificación semiformal, su aplicación en Blockchain*. *Revista Mikarimin*, 10(3), 31–42.

²³ El *Proof of Work (PoW)* es el protocolo de consenso de Bitcoin. Véase Nakamoto, S., *Op cit.*, n

un “notario digital colectivo”, capaz de registrar transacciones de forma transparente, verificable y sin necesidad de que las partes depositen confianza en un tercero.²⁴

Así, de forma simplificada, puede decirse que la blockchain funciona como una secuencia de bloques que recogen distintas transacciones, las cuales son validadas por los participantes del sistema siguiendo unas reglas comunes, y que se van uniendo entre sí de forma que cada nuevo bloque contiene una referencia al anterior, lo que impide modificar el historial sin alterar toda la cadena y garantiza así la seguridad y la transparencia del sistema.

2.2.2. Características jurídico-relevantes de la tecnología blockchain

A partir de su funcionamiento, pueden identificarse una serie de propiedades técnicas esenciales que definen el comportamiento de los criptoactivos basados en blockchain. Estas características, derivadas directamente del diseño del sistema, permiten que las operaciones se realicen de forma autónoma, segura y sin necesidad de intermediarios.²⁵

Entre las más relevantes se encuentran: la descentralización, la replicación de la información entre nodos, la inmutabilidad de los registros, la trazabilidad técnica de las operaciones y la posibilidad de ejecutar transacciones sin intervención de terceros. Estas cualidades permiten que la red funcione de manera coordinada y resistente frente a manipulaciones externas, asegurando la integridad del sistema.

Siguiendo una clasificación funcional común, estas propiedades pueden agruparse en tres grandes ejes: seguridad, descentralización y pseudonimato.²⁶ No obstante, el mismo diseño que proporciona robustez tecnológica plantea también dificultades jurídicas en cuestiones clave como la supervisión pública, la identificación de los participantes o la reversión de operaciones ilícitas. Como señala parte de la doctrina, “las características descritas [...] hacen que las criptomonedas sean altamente seguras a nivel técnico, pero son los mismos rasgos los que las hacen manifiestamente inseguras a nivel delictivo”.²⁷

La **seguridad** del sistema se basa en el uso de funciones hash²⁸ y en la estructura encadenada de los bloques. Cada bloque contiene un sello temporal, los datos de las transacciones y una huella digital (hash) del bloque anterior, lo que permite verificar su integridad y asegurar su correcta vinculación con el resto de la cadena. De este diseño

²⁴ Cereijo Comet, M. (2018). *Análisis de la blockchain y de las criptomonedas: Relación con el delito de blanqueo de capitales* (Trabajo de Fin de Grado, Universidad Pontificia Comillas), p. 31. Disponible en el Repositorio de Comillas [URL]

²⁵ Las criptomonedas no tienen una existencia física ni un respaldo material, por lo que su funcionamiento depende estrictamente de sus atributos y basamentos computacionales.

²⁶ Véase: Navarro Cardoso, F. (2019). *Criptomonedas (en especial, Bitcoin) y blanqueo de dinero*. *Revista Electrónica de Ciencia Penal y Criminología*, (21), pp. 13-16; Domínguez García, J. M., & García Ruiz, R. (2018). *Blockchain y las criptomonedas: el caso Bitcoin*. *Oikonomics*, (10), pp. 60-62. Puede a su vez subclasificarse en características estructurales (inmutabilidad y descentralización) y funcionales (pseudonimato y trazabilidad) Chamorro Rodríguez, M.ª de la C. (Op. Cit., n.)

²⁷ Samar Violeta, F. A., & Olmedo Cardente, M. D. (2024). *Enfoques regulatorios internacionales de las criptomonedas en función del grado de intervención punitiva*. *Cuadernos de Política Criminal*, (143), p. 184.

²⁸ Agencia Española de Protección de Datos & Supervisor Europeo de Protección de Datos. (2019). *Introducción al hash como técnica de seudonimización de datos personales*. https://www.edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_es.pdf

técnico se infiere una propiedad esencial del sistema: la **inmutabilidad** del registro. Una vez validada una transacción e incorporada a la cadena, no puede ser modificada ni anulada sin alterar todos los bloques siguientes, lo que resulta prácticamente inviable desde el punto de vista computacional. Esta arquitectura garantiza la autenticidad de la información sin necesidad de un intermediario de confianza.²⁹

Ahora bien, esta inmutabilidad que aporta seguridad técnica plantea serios límites desde el punto de vista jurídico. Si una operación resulta ser ilícita, por ejemplo, una transferencia vinculada a delitos como el blanqueo de capitales, su cancelación o reversión no depende de una autoridad central ni de ningún operador sujeto a regulación, sino que exige acudir a mecanismos externos, como el rastreo judicial posterior o la cooperación entre jurisdicciones. Tal y como advierte parte de la doctrina,³⁰ esta imposibilidad de intervención directa puede frustrar la restitución de activos, dificultando la reparación del daño y la adopción de medidas cautelares eficaces. La propia estructura técnica de la blockchain, diseñada para resistir manipulaciones, se convierte así en una barrera para la actuación penal y administrativa, especialmente cuando no hay un proveedor de servicios que actúe como punto de control.

La descentralización constituye uno de los principios fundacionales de la tecnología blockchain. A diferencia del sistema financiero tradicional, no existe una autoridad central que controle, verifique o autorice las transacciones. En su lugar, la validación y el almacenamiento de la información se realiza de forma distribuida por una red de nodos independientes, que aplican reglas comunes mediante mecanismos de consenso, como el Proof of Work o el Proof of Stake. Este diseño elimina la necesidad de intermediarios³¹ financieros y otorga al sistema una alta resiliencia técnica frente a manipulaciones, ya que cualquier intento de modificación no consensuado es automáticamente rechazado por la mayoría de los nodos.

Ahora bien, esta arquitectura técnica plantea serias dificultades desde el punto de vista jurídico. En ausencia de una entidad responsable o de un punto de control institucional, se dificulta la supervisión regulatoria, la trazabilidad jurídica de los responsables³² y la ejecución efectiva de medidas de bloqueo o decomiso. Podría pensarse lo mismo del dinero en efectivo que, aunque también es anónimo y descentralizado en su circulación, existe un marco legal claro, intermediarios sujetos a control (bancos, entidades de pago) y una autoridad monetaria que respalda su uso y puede intervenir ante abusos. Por el contrario, en los sistemas blockchain públicos, no hay emisor, custodio ni garante, lo que impide aplicar los instrumentos jurídicos tradicionales y aumenta el riesgo de opacidad y de impunidad operativa, especialmente en contextos como el blanqueo de capitales o la financiación del terrorismo.

A ello se suma el carácter **pseudónimo** del sistema. Las operaciones realizadas en una blockchain pública son, por definición, visibles y accesibles, ya que el registro es transparente y replicado en todos los nodos.³³ Sin embargo, los participantes en estas

²⁹ Navarro Cardoso, F., *op. cit.*, n.

³⁰ Cereijo Comet, *Op. cit.*, n.

³¹ Ibáñez Jiménez, J. W. (2018). *Blockchain: primeras cuestiones en el ordenamiento español*. Dykinson, p. 15.

³² Guardia Civil (2022). *Criptomonedas y blanqueo de capitales*. *Revista Guardia Civil*, nº 265, p. 5.

³³ Navarro Cardoso, F., *Op. cit.*, n.

transacciones no aparecen identificados con nombre y apellidos, sino mediante cadenas alfanuméricas generadas criptográficamente, que actúan como identificadores únicos dentro del sistema.³⁴ Estos identificadores —habitualmente denominados *direcciones públicas*— están asociados a programas o aplicaciones conocidos como *monederos digitales* o *wallets*, los cuales almacenan las claves criptográficas del usuario y permiten gestionar los activos.³⁵ Aunque desde el punto de vista técnico existe una trazabilidad total del recorrido de los fondos, esta no se traduce necesariamente en una trazabilidad jurídica, ya que no existe una correspondencia inmediata entre dirección pública,³⁶ y persona física o jurídica.

A diferencia del dinero en efectivo, cuya opacidad es total pero limitada al ámbito físico, el pseudonimato de las criptomonedas permite realizar operaciones transfronterizas y automatizadas sin identificar al titular real, salvo que se utilicen plataformas reguladas. Esto genera un espacio de anonimato funcional en entornos digitales, donde las autoridades pueden seguir el rastro de las transacciones, pero no vincularlo fácilmente con una identidad concreta. Esta asimetría entre trazabilidad técnica y opacidad jurídica constituye uno de los principales desafíos para la prevención y persecución del blanqueo de capitales en el entorno cripto.

En definitiva, las propiedades técnicas analizadas constituyen elementos esenciales para el funcionamiento de los sistemas basados en blockchain. A nivel técnico, estas características garantizan la autonomía operativa, la resistencia frente a manipulaciones externas y la veracidad del registro de transacciones. Precisamente por estar diseñadas para asegurar un entorno informático robusto y autónomo, estas propiedades repercuten directamente en la forma en que las operaciones pueden ser supervisadas, intervenidas o corregidas. Esta conexión entre diseño técnico y consecuencias normativas obliga a considerar que los mecanismos que hacen posible la eficiencia del sistema no se traducen necesariamente en una compatibilidad plena con las exigencias del ordenamiento jurídico.³⁷ Cuestiones como la supervisión institucional, la posibilidad de reversión de operaciones o la identificación de intervinientes resultan profundamente condicionadas por la arquitectura descentralizada de la red.³⁸

La imposibilidad de modificar registros una vez incorporados a la cadena, derivada del uso de funciones hash y del encadenamiento de bloques, impide cualquier actuación *ex post* con efectos restitutorios, incluso cuando las transacciones resulten ilícitas. Esta limitación puede entrar en contradicción con principios jurídicos fundamentales, como el de reparación del daño, y dificulta la aplicación efectiva de medidas correctivas. A ello se suma la inexistencia de un órgano rector capaz de intervenir en tiempo real sobre el sistema, lo que traslada la respuesta institucional a mecanismos externos, como el rastreo de activos o la cooperación internacional.³⁹

La trazabilidad de las operaciones en redes públicas no elimina un elemento de opacidad significativo: el pseudonimato. Las direcciones alfanuméricas que identifican a los

³⁴ Chamorro Rodríguez, M.^ª de la C., *Op. cit.*, n

³⁵ Guardia Civil, *Op. cit.*, n.

³⁶ Chamorro Rodríguez, M.^ª de la C., *Op. cit.*, n.

³⁷ Samar Violeta y Olmedo Cardente, *Op. cit.*, n

³⁸ Chamorro Rodríguez, M.^ª de la C., *Op. cit.*, n.

³⁹ Navarro Cardoso, F., *Op. cit.*, n.

usuarios, generadas criptográficamente, no permiten establecer de forma directa la identidad de los titulares reales. Esta limitación no es del todo nueva, pues tampoco el dinero en efectivo es un bien nominativo: billetes y monedas no permiten identificar al portador, lo que ha sido históricamente aprovechado en operaciones opacas. Sin embargo, el riesgo en el entorno cripto se agrava por la posibilidad de realizar transferencias transfronterizas instantáneas, sin intermediarios ni puntos de contacto regulados, lo que dificulta notablemente la intervención institucional. Esta estructura facilita, en determinados contextos, la creación de esquemas que escapan al control normativo y pueden favorecer la criminalidad organizada.⁴⁰

Estas propiedades, concebidas para garantizar el funcionamiento autónomo y seguro del sistema, son las mismas que permiten, en la práctica, que los criptoactivos puedan ser empleados como instrumentos para actividades fraudulentas. En particular, su potencial para dificultar la trazabilidad jurídica y obstaculizar la intervención institucional los convierte en una herramienta especialmente apta para esquemas de blanqueo de capitales. Así lo subraya también la doctrina más reciente, al señalar que la configuración técnica de estos activos, unida a la falta de una infraestructura regulatoria sólida, facilita su utilización en operaciones que buscan eludir los mecanismos tradicionales de control financiero.⁴¹ A partir de esta premisa, los epígrafes siguientes abordarán las implicaciones específicas de estas características en el contexto del delito de blanqueo y su encaje dentro del marco penal y administrativo vigente.

2.3. El ecosistema de las criptomonedas: usuarios, transacciones, wallets y exchanges

El ecosistema está conformado por todos aquellos elementos que intervienen en el sistema y se interrelacionan entre sí. Entre ellos se encuentran los usuarios, las transacciones, las carteras o monederos digitales (*wallets*) y las plataformas de intercambio (*exchanges*).

Dado que el funcionamiento de los nodos y las transacciones ya ha sido tratado en apartados anteriores, aquí se abordarán exclusivamente los *wallets* y *exchanges*, por considerarlos especialmente relevantes para comprender el funcionamiento práctico del sistema y los riesgos que pueden derivarse de su utilización.

El propósito es ofrecer una visión general que facilite la comprensión del sistema cripto y sirva de base para el análisis posterior de los riesgos asociados. Cabe señalar que la estructura del ecosistema descrita no responde exclusivamente a una criptomoneda en particular, aunque resulta especialmente característica del sistema de Bitcoin por ser el primero y más representativo. Sin embargo, los elementos analizados —usuarios, transacciones, *wallets* y *exchanges*— se encuentran, con ciertas variaciones, en la mayoría de criptomonedas existentes. Estas diferencias pueden derivar del grado de

⁴⁰ Ibid., p.

⁴¹ Véase, por ejemplo: Adrian, T., & Mancini-Griffoli, T. (2021). *A New Era of Digital Money*. Fondo Monetario Internacional (IMF), <https://www.imf.org/external/pubs/ft/fandd/2021/06/online/digital-money-new-era-adrian-mancini-griffoli.htm>. Financial Action Task Force (FATF). (2020). *Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing*, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html>

descentralización del sistema, de la existencia o no de una entidad emisora, o de la tecnología empleada, como ocurre en los criptoactivos basados en contratos inteligentes o en las *stablecoins*. Por tanto, en este trabajo se adopta una visión estructural generalizada, útil para comprender el funcionamiento básico del ecosistema cripto en su conjunto.

2.3.1. Monederos digitales (*wallets*)

Los monederos digitales, también conocidos como *wallets*, constituyen una herramienta esencial en el ecosistema cripto, ya que permiten gestionar las claves necesarias para operar con criptomonedas. Contrariamente a la creencia común, en estos monederos no se almacenan las criptomonedas en sí, sino las claves privadas y públicas ⁴² asociadas a las direcciones de la cadena de bloques. El acceso a los fondos depende, por tanto, de la custodia segura de esas claves, especialmente de la clave privada, que otorga el control sobre los activos vinculados a una dirección concreta.⁴³

Existen múltiples tipos de *wallets*, que pueden clasificarse principalmente según su nivel de conexión a Internet: *cold wallets* (monederos fríos) y *hot wallets* (monederos calientes). Las *cold wallets* operan *offline*, lo que ofrece una mayor seguridad frente a ataques cibernéticos. Dentro de esta categoría se encuentran las *hardware wallets*, dispositivos físicos diseñados específicamente para almacenar claves (como Trezor o Ledger),⁴⁴ así como las *paper wallets*, que consisten en copias físicas de las claves impresas en papel.⁴⁵

En contraste, las *hot wallets* requieren conexión constante a Internet, lo que facilita su uso cotidiano pero aumenta su vulnerabilidad ante ciberataques. Estas incluyen las *wallets* de escritorio, móviles y web. Algunas versiones, como los *full clients*,⁴⁶ permiten al usuario participar activamente en la red como nodo y realizar una verificación completa de las transacciones; otras, como las *SPV wallets*,⁴⁷ permiten una verificación simplificada de

⁴² En los sistemas basados en blockchain, cada usuario posee un par de claves: una **clave pública**, que funciona como una dirección visible y sirve para recibir fondos, y una **clave privada**, que se utiliza para firmar transacciones y acceder a los activos. La clave privada debe mantenerse secreta, ya que quien la posea puede disponer de los fondos asociados a su correspondiente clave pública. Véase Antonopoulos, A. M. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (2.ª ed.). O'Reilly Media. Citado en: Saldaña Taboada, P. (2023). *Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes* (Tesis doctoral, Universidad de Granada), p. 95. <https://hdl.handle.net/10481/81413>

⁴³ Ibid.

⁴⁴ Son marcas comerciales concretas de *hardware wallets*

⁴⁵ Saldaña Taboada, P. (2023). *Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes* (Tesis doctoral, Universidad de Granada). <https://hdl.handle.net/10481/81413>

⁴⁶ Los “*full clients*” (clientes completos) son programas que almacenan una copia íntegra de la cadena de bloques y validan todas las transacciones de forma autónoma, lo que los convierte en nodos completos dentro de la red.

⁴⁷ Las “*SPV wallets*” (Simplified Payment Verification) son monederos ligeros que permiten verificar pagos de forma simplificada al conectarse a nodos completos de la red, sin necesidad de descargar toda la cadena de bloques.

las transacciones sin necesidad de descargar toda la cadena de bloques, lo que reduce su autonomía pero mejora la eficiencia para usuarios con recursos limitados.⁴⁸

La elección del tipo de *wallet* dependerá del perfil del usuario y del uso que pretenda dar a las criptomonedas: mientras que las *hot wallets* se asemejan al efectivo por su facilidad de uso, las *cold wallets* se emplean más comúnmente como herramientas de almacenamiento seguro a largo plazo. En consecuencia, el diseño y uso de los wallets tiene un impacto directo en los riesgos asociados a la custodia de criptoactivos, ya que permiten gestionar fondos sin necesidad de intermediarios regulados y sin vinculación directa a la identidad del usuario. Al operar mediante direcciones pseudónimas, tanto los hot como los cold wallets pueden ser utilizados para ocultar la titularidad real de los activos y dificultar su rastreo, especialmente cuando se combinan con técnicas como los mixers o los intercambios en plataformas descentralizadas. Esta opacidad técnica convierte a los wallets en un instrumento potencialmente útil en esquemas de ocultación patrimonial y blanqueo de capitales..⁴⁹

2.3.2. *Exchanges*

Las plataformas de intercambio de criptomonedas, también denominadas *exchanges*, son infraestructuras digitales que permiten comprar, vender, intercambiar o convertir criptoactivos, tanto entre diferentes criptomonedas como respecto a monedas de curso legal (fiat)⁵⁰. Actúan como intermediarios entre usuarios, facilitando la operativa mediante herramientas similares a las de los mercados financieros tradicionales.

Los *exchanges* pueden dividirse en tres grandes categorías: plataformas de clearing, plataformas centralizadas (CEX) y plataformas descentralizadas (DEX).⁵¹ En las *clearing*, la plataforma realiza una función de verificación pero no llega a custodiar los fondos; en las centralizadas, es la propia empresa operadora la que actúa como depositaria tanto de los criptoactivos como de la información del usuario. Este último modelo facilita la experiencia del usuario y mejora la liquidez, pero conlleva riesgos evidentes relacionados con el control efectivo de los fondos, la vulnerabilidad ante ciberataques o la falta de transparencia.⁵²

Por su parte, las plataformas descentralizadas (DEX) no dependen de una entidad intermediaria. Operan mediante contratos inteligentes, lo que permite que los usuarios conserven el control de sus claves privadas y realicen operaciones de forma directa y autónoma. Si bien ofrecen mayores garantías en cuanto a privacidad y descentralización, requieren conocimientos técnicos más avanzados y presentan, en ocasiones, menor liquidez y usabilidad.⁵³

El papel que desempeñan los *exchanges* en el ecosistema cripto es crucial, ya que constituyen el principal punto de conexión entre el sistema financiero tradicional y el sistema blockchain. Por esta razón, el legislador europeo ha comenzado a aplicar sobre

⁴⁸ Antonopoulos, A. M. (2017), citado en Saldaña Taboada, P. (2023), p. 97.

⁴⁹ Saldaña Taboada, *op. cit.*

⁵⁰ Saldaña Taboada, *op. cit.*

⁵¹ Pieters, G., & Vivanco, S. (2015). *Bitcoin arbitrage and unofficial exchange rates*. Citado en Saldaña Taboada, P. (2023), p. 100.

⁵² Saldaña Taboada, *op. cit.*

⁵³ Pieters, G., & Vivanco, S., *op. cit.*

ellos medidas propias del sector financiero tradicional, como las obligaciones de identificación (Know Your Customer. “KYC”) y diligencia debida, en virtud de la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo.⁵⁴ Esta incorporación normativa responde a la necesidad de limitar el grado de anonimato que históricamente ha caracterizado a muchas operaciones en exchanges, especialmente en aquellos no regulados o ubicados fuera del espacio europeo. Dado que estas plataformas permiten la conversión directa entre criptoactivos y dinero fiduciario, sin controles efectivos podrían facilitar la entrada y salida de fondos ilícitos en el sistema económico legal. Por ello, las obligaciones KYC resultan esenciales para garantizar la trazabilidad jurídica de las transacciones, identificar a los titulares reales y prevenir su utilización con fines de blanqueo de capitales o financiación del terrorismo. Estas obligaciones resultan clave para su consideración dentro de los mecanismos de prevención del blanqueo de capitales, así como para garantizar una mayor trazabilidad de las operaciones, cuestión que será abordada más adelante con mayor profundidad.

2.4. La aproximación jurídica a las criptomonedas: retos conceptuales y normativos

La calificación jurídica de las criptomonedas ha generado, desde sus primeras manifestaciones, un debate constante derivado de su difícil encaje en las categorías tradicionales del Derecho patrimonial y financiero. Esta dificultad responde a su naturaleza descentralizada, su complejidad tecnológica y su pluralidad funcional, lo que las aleja de los instrumentos jurídicos clásicos y complica su tratamiento normativo unitario.

El legislador europeo ha optado por una aproximación funcional y abierta, evitando definir jurídicamente la “criptomonedas” y adoptando en su lugar el concepto más amplio de criptoactivo, definido por el artículo 3 del Reglamento (UE) 2023/1114 (MiCA) como *“una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente mediante tecnología de registro distribuido o una tecnología similar”*⁵⁵. Este enfoque permite abarcar una gran diversidad de activos, pero no incluye los instrumentos financieros regulados por MiFID II⁵⁶, el dinero electrónico, los productos de seguros, los sistemas de pensiones ni los activos no fungibles (como los NFTs o determinados tokens vinculados a bienes singulares)⁵⁷ u otros tokens vinculados a bienes singulares. Así, el marco normativo europeo establece una definición negativa, delimitando el ámbito de aplicación del Reglamento no tanto por lo que los criptoactivos son, sino por lo que no son.

⁵⁴ Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849. DOUE L 156, 19.6.2018.

⁵⁵ Reglamento (UE) 2023/1114, op. cit., art. 2.

⁵⁶ Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros, por la que se modifica la Directiva 2002/92/CE y la Directiva 2011/61/UE. *Diario Oficial de la Unión Europea*, L 173, 12 de junio de 2014, pp. 349–496. Conforme a ella, ciertos criptoactivos pueden adquirir la condición de instrumentos financieros cuando incorporan derechos patrimoniales, participativos o de renta fija.

⁵⁷ Reglamento (UE) 2023/1114, op. cit., art. 2.

En paralelo a los intentos normativos, la doctrina ha formulado diversas propuestas para encajar jurídicamente las criptomonedas. Una corriente las considera bienes patrimoniales digitales inmateriales, susceptibles de integrarse en el tráfico jurídico privado como objeto de permuta, pero no como dinero legal⁵⁸. Otras posturas proponen su asimilación a activos financieros o valores mobiliarios, especialmente en el caso de ciertos tokens que otorgan derechos económicos o de gobernanza. Sin embargo, estas clasificaciones presentan limitaciones: la ausencia de un emisor identificable, la falta de garantía institucional y la liquidez restringida de muchas criptomonedas impiden su equiparación plena con las figuras tradicionales del Derecho financiero.

En consecuencia, más que una categoría jurídica cerrada, la criptomoneda debe entenderse como un fenómeno en evolución, cuya regulación normativa aún se encuentra en fase de consolidación⁵⁹. El presente trabajo no busca resolver este debate, sino analizar su utilización en esquemas de blanqueo y la suficiencia del marco normativo para responder eficazmente a estos riesgos.

2.3.3. *Las criptomonedas como bienes en el Derecho español*

En ausencia de una normativa específica que regule de forma positiva la naturaleza jurídica de las criptomonedas, el análisis debe partir del marco general del Derecho patrimonial y civil español. Desde este enfoque, se ha consolidado la tesis de que las criptomonedas, pese a su intangibilidad y falta de respaldo institucional, pueden ser calificadas como bienes muebles inmateriales dotados de valor económico y susceptibles de integración en el tráfico jurídico.

La jurisprudencia ha ofrecido un primer apoyo a esta consideración. La Sentencia del Tribunal Supremo 326/2019, de 20 de junio, reconoció expresamente que el bitcoin constituye un activo patrimonial inmaterial, definido mediante tecnología informática y criptográfica, cuyo valor se determina por la dinámica del mercado⁶⁰. Esta aproximación ha sido respaldada por diversas construcciones doctrinales que, desde una lectura sistemática del Código Civil —especialmente de sus artículos 333, 335 y 337—, permiten afirmar que los cryptoactivos reúnen los requisitos esenciales para ser calificados como bienes:⁶¹ son individualizables, apropiables, transferibles y tienen un valor económico reconocible.

La amplitud del concepto jurídico de “bien” en el Derecho civil español admite la inclusión de entidades digitales que, aun sin materialidad física, puedan formar parte del patrimonio de los sujetos. Esta condición se ve reforzada por el hecho de que las criptomonedas pueden ser objeto de relaciones contractuales, ser aportadas como bienes no dinerarios a sociedades, embargadas en procesos judiciales o transmitidas inter vivos. La configuración tecnológica que las sustenta —mediante blockchain y redes descentralizadas— no altera su carácter jurídico esencial como objetos patrimoniales.⁶²

⁵⁸ Puente González, I. A. (2020). *Criptomonedas y Derecho civil patrimonial*. Diario La Ley, (9619), p. 29.

⁵⁹ Ramos Gil de la Haza, A. (2022). La web3: una aproximación jurídica. *Revista Jurídica Pérez-Llorca*, (8), p. 24.

⁶⁰ Tribunal Supremo, Sala Segunda. (2019). *Sentencia nº 326/2019, de 20 de junio*. (FJ 3)

⁶¹ Véase Código Civil español, arts. 333, 335 y 337.

⁶² Schuller, R. R., *Cryptoactivos: Categorización jurídica de los cryptoactivos e introducción a la tecnología DLT/Blockchain*, Cuadernos de Derecho Transnacional, vol. 14, nº 2, 2022, pp. 1129–1145.

Esta calificación resulta de particular relevancia para el presente trabajo, ya que habilita el tratamiento de las criptomonedas como objeto material del delito de blanqueo de capitales. Su consideración como bienes patrimoniales permite afirmar que pueden ser adquiridas, poseídas, transmitidas y ocultadas en el contexto de operaciones ilícitas, de modo que el Derecho penal puede operar sobre ellas con la misma lógica que sobre cualquier otro activo susceptible de incorporación al patrimonio.

En definitiva, la calificación de las criptomonedas como bienes patrimoniales muebles inmateriales no solo permite su integración en el tráfico jurídico civil, sino que las convierte en susceptibles de ser objeto de blanqueo de capitales, al ser apropiables, transmisibles y, a la vez, opacas en su circulación. Precisamente esta conjunción de valor económico y dificultad de rastreo las hace particularmente idóneas para ser utilizadas en esquemas de ocultación patrimonial. Aunque el Tribunal Supremo ya se ha pronunciado sobre el carácter patrimonial del bitcoin, resultaría deseable una mayor clarificación jurisprudencial respecto del resto de cryptoactivos, especialmente en lo relativo a su consideración como objeto del delito y a los efectos jurídicos derivados de su uso en operaciones ilícitas.

3. REGULACIÓN DEL BLANQUEO DE CAPITALS

3.1. Concepto

El delito de blanqueo de capitales, cuya configuración jurídica se consolidó a partir de la Convención de Viena de 1988, ha experimentado una progresiva ampliación en su alcance desde su vinculación originaria con el narcotráfico hacia un concepto más amplio que abarca cualquier operación destinada a dar apariencia de legalidad a bienes de procedencia ilícita.

Existen diversas definiciones según el enfoque adoptado: desde una perspectiva internacional, el Grupo de Acción Financiera Internacional sobre el Blanqueo de Capitales (GAFI), un organismo intergubernamental cuyo propósito es elaborar y promover medidas para combatir el blanqueo de capitales y financiación del terrorismo, lo concibe como la conversión de activos con el fin de enmascarar su origen delictivo y eludir las consecuencias legales, poniendo el acento en la transformación de bienes ilícitos en activos de tráfico legal.⁶³ En el ámbito nacional, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (CPBCIM) lo define como toda actividad dirigida a ocultar el origen ilícito de unos bienes concretos para introducirlos en el circuito económico simulando su licitud, destacando la doble operación de transformación y legitimación.⁶⁴ Algunos enfoques académicos lo presentan como toda acción orientada a dar apariencia legal a capitales ilícitos, incluso abriendo el debate doctrinal sobre la amplitud interpretativa del tipo penal, al incluir actos que “no se

⁶³ Grupo de Acción Financiera Internacional (GAFI), *Glosario de términos clave*, disponible en: <https://www.fatf-gafi.org> [consulta: 3 mayo 2025].

⁶⁴ Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (CPBCIM), *Guía sobre el delito de blanqueo de capitales y su prevención*, Ministerio de Asuntos Económicos y Transformación Digital, 2021.

limitan” a los específicamente descritos en la norma⁶⁵. En términos técnico-jurídicos, puede entenderse como el proceso mediante el cual los bienes provenientes de actividades delictivas se integran en el sistema económico formal con una apariencia de licitud que oculta su verdadero origen.⁶⁶

En definitiva, el blanqueo de capitales puede definirse como el conjunto de operaciones orientadas a ocultar el origen delictivo de determinados bienes, con el fin de incorporarlos al tráfico económico legal y conferirles una apariencia lícita.

Esta lógica delictiva resulta especialmente compatible con las propiedades técnicas de las criptomonedas, tal y como se ha analizado en los apartados anteriores. La opacidad estructural derivada del pseudonimato, la ausencia de intermediarios identificables y la descentralización del sistema blockchain dificultan la detección del origen ilícito de los fondos y obstaculizan las labores de supervisión. Por ello, las criptomonedas se configuran como activos especialmente idóneos para las operaciones de blanqueo, al permitir canalizar capitales ilícitos hacia el circuito económico legal mediante estructuras que resisten los mecanismos tradicionales de control. Esta compatibilidad entre el diseño técnico de los cryptoactivos y los fines típicos del delito de blanqueo constituye uno de los principales desafíos actuales del Derecho penal económico.

3.2. Evolución y fundamentos normativos

La lucha contra el fenómeno del blanqueo de capitales se articula en el ordenamiento jurídico español a través de una doble vertiente: por un lado, como conducta delictiva y, por otro, como infracción administrativa. Con el objetivo de prevenir estas conductas, el legislador ha optado no solo por sancionar su comisión, sino también por anticiparse a su aparición, estableciendo mecanismos de control y prevención en una fase previa. En este sentido, el ilícito penal se encuentra tipificado en el artículo 301 del Código Penal, mientras que la vertiente administrativa se regula en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Ambas configuraciones comparten el fin de proteger la integridad del sistema financiero y combatir la criminalidad económica, pero operan en planos normativos distintos: la penal reprime conductas consumadas, mientras que la administrativa impone deberes ex ante de diligencia, vigilancia y colaboración. Esta distinción se refleja también en el sujeto activo: el ilícito penal puede ser cometido por cualquier persona, mientras que el ilícito administrativo solo puede ser imputado a los sujetos obligados previstos en la Ley 10/2010, quienes, por su posición dentro del sistema financiero, ostentan una capacidad de control, intermediación o supervisión sobre flujos económicos que justifica la imposición de deberes específicos de detección, comunicación y prevención del riesgo de blanqueo.

⁶⁵ Del Carpio Delgado, J., “Sobre la necesaria interpretación y aplicación restrictiva del delito de blanqueo de capitales”, *InDret*, n.º 4/2016, Universidad Pablo de Olavide, disponible en www.indret.com.

⁶⁶ Blanco Cordero, I., *El delito del blanqueo de capitales*, Aranzadi, 4.ª ed., Pamplona, 2015, p. 107.

3.3. Naturaleza penal del blanqueo de capitales: el artículo 301 del Código Penal

El artículo 301 del Código Penal configura el delito de blanqueo como una figura compleja y expansiva, orientada a impedir la introducción en el circuito económico legal de bienes procedentes de actividades delictivas. Castiga al que, “*sabiendo que los bienes tienen su origen en una actividad delictiva*”, los adquiera, posea, utilice, convierta, transmita o realice cualquier otro acto para ocultar su origen ilícito o ayudar a eludir sus consecuencias legales.⁶⁷

Se trata de un tipo penal configurado con una redacción amplia y flexible, que permite abarcar conductas diversificadas y esquemas técnicamente sofisticados, como los que se desarrollan en el entorno digital de los criptoactivos⁶⁸ Esta amplitud ha sido objeto de crítica doctrinal, al considerar que el tipo se ha convertido en un “auténtico cajón de sastre”, capaz de albergar comportamientos muy diversos y, en ocasiones, alejados del núcleo de ilicitud que justifica una sanción penal.⁶⁹

El precepto admite además la comisión por imprudencia grave, especialmente aplicable a personas jurídicas y sujetos obligados, reforzando su papel preventivo⁷⁰. Su diseño se alinea con los estándares internacionales fijados por el GAFI, la Convención de Viena (1988) y la Directiva (UE) 2018/1673, que han promovido un enfoque estructural y no meramente accesorio del blanqueo.⁷¹

3.3.1. Bien jurídico protegido

El delito de blanqueo de capitales protege, de forma principal, la integridad del sistema económico y financiero, entendida como la legalidad, transparencia y fiabilidad del tráfico patrimonial. El objetivo es evitar que los beneficios obtenidos a través de actividades delictivas se introduzcan en el circuito económico legal con apariencia de licitud.⁷²

En la doctrina y la jurisprudencia se han formulado tres grandes enfoques sobre el bien jurídico protegido. El primero, más restrictivo, sostiene que lo protegido es la administración de justicia, en la medida en que el blanqueo dificulta la persecución del delito antecedente. El segundo enfoque, hoy mayoritario, considera que el bien jurídico es el orden socioeconómico, especialmente la confianza en el sistema financiero y la transparencia del mercado.⁷³

⁶⁷ Código Penal español, art. 301

⁶⁸ Blanco Cordero, *op. cit.*

⁶⁹ Del Carpio Delgado, *op. cit.*

⁷⁰ Muñoz Conde, *op. cit.*

⁷¹ Palma Herrera, *op. cit.*

⁷² Ley 10/2010, de prevención del blanqueo de capitales, art. 1.1 – “protección de la integridad del sistema financiero” – *op. cit.*

⁷³ Muñoz Conde, *op. cit.*

Finalmente, una tercera posición adopta una perspectiva pluriofensiva, señalando que el delito de blanqueo lesiona de forma simultánea varios bienes jurídicos, más allá del económico. Así, Doval País identifica como bienes protegidos:

- El bien jurídico lesionado por el delito previo
- La administración de justicia
- El orden económico
- El orden social
- La seguridad nacional o interior del Estado
- La estabilidad institucional y la democracia
- El correcto funcionamiento de los mercados financieros⁷⁴

Esta visión integradora ha sido recogida por la jurisprudencia del Tribunal Supremo, que ha afirmado que el tipo penal sanciona cualquier actuación que contamine el sistema económico con capitales ilícitos, comprometiendo tanto la justicia penal como el tráfico patrimonial.⁷⁵

En el ámbito de los criptoactivos, esta dimensión estructural del bien jurídico cobra especial relevancia. La descentralización, el pseudonimato y la falta de intermediarios tradicionales dificultan la identificación del origen de los fondos y agravan el riesgo de lesión del bien protegido. Así, aunque el artículo 301 CP mantiene la misma finalidad protectora, las características técnicas del ecosistema cripto exigen una respuesta jurídico-penal más exigente y adaptativa.⁷⁶

3.3.2. Elementos del tipo

Como ocurre en todo tipo penal, la configuración del delito de blanqueo de capitales se articula en torno a elementos objetivos, subjetivos y un objeto material. Sin embargo, en este caso, el objeto material adquiere una relevancia central, hasta el punto de erigirse en el elemento nuclear del tipo. Por esta razón, y con el fin de facilitar una adecuada comprensión dogmática, el análisis se iniciará precisamente por este componente.

a. Objeto material: el origen delictivo de los bienes

De forma general, puede entenderse por objeto material aquel elemento, persona o cosa, sobre la que recae la conducta típica⁷⁷. En el delito de blanqueo de capitales, conforme a lo dispuesto en el artículo 301 del Código Penal, la conducta recae sobre “bienes” y más en concreto, sobre bienes con origen delictivo.

Es preciso, por tanto, determinar qué debe entenderse por bienes y, en segundo lugar, su origen delictivo.

⁷⁴ Doval País, *op. cit.*

⁷⁵ STS 56/2014, de 6 de febrero, FJ 2.º: “[...] el interés del Estado en controlar el flujo de capitales procedentes de actividades delictivas ejecutadas a gran escala y que pueden menoscabar el sistema económico, afectando también al buen funcionamiento del mercado y de los mecanismos financieros y bursátiles”.

⁷⁶ Pérez López, *op. cit.*

⁷⁷ Cizur Menor: Aranzadi, p. 232. Orts Berenguer, E.; González Cussac, J. (2020) “Introducción al Derecho Penal. Parte general”, Valencia: Tirant lo Blanch, p. 152.

En el contexto del delito de blanqueo de capitales, el concepto de "bienes" debe interpretarse de manera amplia y conforme a los estándares internacionales. La Directiva 91/308/CEE, en su artículo 10, y la Convención de Viena de 1988, en su artículo 1.q, coinciden en definir los bienes como cualquier tipo de activo, abarcando los materiales, inmateriales, muebles o inmuebles, tangibles o intangibles. Esta definición incluye también los documentos o instrumentos legales que acrediten derechos de propiedad o intereses sobre tales activos. En la misma línea, el Convenio Europeo de 1990 incorpora una formulación similar. Desde una perspectiva penal, los bienes pueden entenderse como cualquier ventaja susceptible de valoración económica.⁷⁸

Respecto al origen delictivo, es una cuestión que, aunque aparentemente clara, ha generado importantes en la doctrina penal, tanto en relación con el alcance de esta expresión, es decir, qué tipo de conducta previa puede considerarse idónea para dar origen a un delito de blanqueo, como en torno a su relevancia dentro de la estructura del tipo penal, en particular sobre si debe entenderse como un elemento constitutivo del delito o como una condición objetiva de punibilidad.

En cuanto a la primera cuestión, la interpretación mayoritaria entiende que la actividad delictiva previa ha de consistir en una conducta típicamente antijurídica, aunque no sea necesario que exista una sentencia firme condenatoria ni que se haya identificado al autor del hecho. En consecuencia, se excluyen expresamente las infracciones administrativas o los meros incumplimientos contractuales, ya que carecen de entidad penal. Desde esta perspectiva, lo determinante es que los bienes procedan de una infracción penal sustantiva, aunque no formalmente declarada por una resolución judicial definitiva.⁷⁹

El segundo eje del debate gira en torno a si el delito antecedente constituye un verdadero elemento del tipo o si debe considerarse una condición objetiva de punibilidad. Para quienes adoptan la primera posición, es imprescindible que el sujeto conozca la existencia del delito previo, ya que este conocimiento forma parte del dolo. Por el contrario, si se entiende que se trata de una condición objetiva, bastaría con que la actividad delictiva se haya producido, independientemente del conocimiento del autor. Palma Herrera, en una posición intermedia, considera que basta con acreditar que los bienes proceden de una conducta típica y antijurídica, aunque no exista una declaración formal sobre su ilicitud ni se haya determinado la responsabilidad del autor del delito fuente.⁸⁰

Esta interpretación ha sido recogida y desarrollada por la jurisprudencia del Tribunal Supremo. En particular, la STS 928/2006 exige una “identificación suficiente” del origen delictivo de los bienes, lo que implica que, sin necesidad de una calificación jurídica precisa ni de una condena firme⁸¹, deben aportarse elementos objetivos que permitan

⁷⁸ Muñoz Conde, F. (2012). *Derecho Penal. Parte especial* (3.ª ed.). Valencia: Tirant lo Blanch. Véase también: Consejo de la Unión Europea. (1991). *Directiva 91/308/CEE del Consejo, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales*. Diario Oficial de las Comunidades Europeas, L 166/77; Naciones Unidas. (1988). *Convención contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas* (Convención de Viena), art. 1.q; Consejo de Europa. (1990). *Convenio relativo al blanqueo, detección, embargo y decomiso de los productos del delito*, art. 1.

⁷⁹ Blanco Cordero, *op. cit.*, p. 508 y ss.

⁸⁰ Palma Herrera, J. M. (2000). *Los delitos de blanqueo de capitales*. Edersa.

⁸¹ Vid. SSTs 501/2019, de 24 de octubre (RJ 2019/501); 4523/2021 (RJ 2021/4523); y 2456/2022, de 16 de junio (RJ 2022/2456).

concluir razonablemente que los bienes provienen de un delito penalmente relevante. En esa misma línea, se descarta expresamente que puedan considerarse como base del blanqueo infracciones administrativas o actividades ilícitas en sentido amplio que no alcanzan el umbral de ilicitud penal.⁸²

Desde el punto de vista subjetivo, la jurisprudencia también ha matizado el estándar exigido. Así, en la STS 2410/2001 se afirma que no es necesario un conocimiento preciso del delito precedente. Basta con una sospecha razonable, fundada en elementos objetivos, como la cuantía del bien, su desproporción respecto a la situación económica del sujeto, la opacidad de la operación o la falta de justificación. Esta concepción permite imputar responsabilidad por blanqueo incluso en casos en los que el autor no tenga certeza sobre la naturaleza exacta del delito fuente, siempre que tenga conciencia de su probable ilicitud.⁸³

Por tanto, puede afirmarse que la exigencia de una actividad delictiva previa no constituye una mera condición externa, sino un elemento estructural del tipo penal, que determina tanto su configuración dogmática como su ámbito de aplicación. Esta interpretación se refuerza en el contexto actual de operaciones con criptoactivos, donde la descentralización, la opacidad y el pseudonimato dificultan el rastreo del origen de los fondos. No obstante, estas dificultades técnicas no pueden justificar una flexibilización del estándar jurídico, ni tampoco una expansión excesiva del tipo penal que vulnere los principios de legalidad y seguridad jurídica. Al contrario, la operativa con activos virtuales exige una aplicación rigurosa y técnicamente informada del concepto de “origen delictivo”, que permita mantener la coherencia del sistema penal sin renunciar a su eficacia frente a nuevas formas de criminalidad financiera.

b. Elemento objetivo: la conducta típica

El artículo 301 del Código Penal incorpora una enumeración de conductas que permiten identificar distintas formas de intervención sobre bienes de origen ilícito. En el contexto actual, muchas de estas conductas encuentran un nuevo campo de aplicación en el uso de criptoactivos. Así, acciones como adquirir, poseer, utilizar o convertir bienes adquieren nuevas formas cuando se realizan a través de transacciones descentralizadas, wallets digitales o plataformas de intercambio de criptomonedas. Esta conexión entre el tipo penal clásico y las operaciones con criptoactivos exige interpretar estas conductas desde una perspectiva tecnológica actualizada, sin perder de vista su contenido jurídico esencia. Con el objetivo de fijar el alcance y límite del delito, procede hacer una breve delimitación de las mismas. De esta manera, el tipo penal establece: “el que adquiera, posea, utilice, convierta, o transmita bienes [...], o realice cualquier otro acto”

- **Adquirir:** Implica la incorporación de un bien o derecho al patrimonio del sujeto, sin importar el título o causa jurídica de esa adquisición. La inclusión de este verbo en instrumentos internacionales como la Convención de Viena

⁸² Tribunal Supremo, Sala de lo Penal. (2006). *Sentencia 928/2006, de 5 de octubre* (RJ 2006/6937), FJ 11.º.

⁸³ Tribunal Supremo, Sala de lo Penal. (2001). *Sentencia 2410/2001, de 18 de diciembre* (RJ 2001/10457), FJ 4.º. Tribunal Supremo, Sala de lo Penal. (2000). *Sentencia 1637/2000, de 10 de enero* (RJ 2000/1637), FJ 5.º.

(1988, art. 3.1.c) y la Directiva 91/308/CEE (art. 1.c, ap. 3.º) refuerza su carácter esencial en la lucha contra el blanqueo. En este contexto, no se exige una *traditio* formal en sentido civil para considerar consumado el delito, sino que basta con cualquier forma de apropiación efectiva, ya sea material o jurídica, que implique la incorporación del bien de origen ilícito al patrimonio del sujeto activo. Esta lectura responde a una lógica teleológica del tipo penal, centrada no en la formalidad del negocio jurídico, sino en el resultado económico-criminal de la operación. La doctrina ha señalado que exigir una transmisión formal restringiría de forma injustificada el alcance del tipo y dejaría fuera numerosos supuestos de blanqueo que se materializan a través de estructuras económicas informales o con apariencia legal⁸⁴.

En relación a los criptoactivos, esta conducta puede manifestarse, por ejemplo, en la compra de criptomonedas a través de exchanges con fondos en efectivo de origen ilícito, o mediante operaciones P2P que evitan cualquier control institucional, dificultando así el rastreo del origen patrimonial.

- **Poseer:** En el marco del artículo 301.1 del Código Penal, la posesión debe entenderse como la situación de poder de hecho sobre un bien, con independencia de que se fundamente o no en un derecho real legítimo. Conforme al artículo 438 del Código Civil, esta figura implica una tenencia que puede revestir distintos grados de intensidad y que permite al poseedor ejercer, de manera provisionalmente prevalente, determinadas facultades sobre la cosa: desde su simple retención hasta el uso, disfrute o mejora, en función del tipo de derecho que se exteriorice (propiedad, usufructo, arrendamiento, etc.). Tal como señala Peña Bernaldo de Quirós, lo definitorio de la posesión es la posibilidad jurídica de mantener la cosa bajo control inmediato y ejercer sobre ella actos de dominio, aunque no se ostente un título formal de propiedad.⁸⁵

La inclusión del verbo “poseer” como conducta típica del delito de blanqueo permite sancionar situaciones en las que el sujeto, aun sin adquirir el bien o explotarlo activamente, lo retiene de manera consciente y voluntaria. De este modo, el control fáctico sobre un bien de origen ilícito, cuando se conoce su procedencia, se erige como una forma autónoma de intervención punible. Lo relevante no es tanto el ejercicio de un uso activo del bien, sino el dominio que se ejerce sobre él desde una posición de control material o jurídico.

En el ámbito cripto, poseer implica el control efectivo sobre una dirección pública o wallet digital que contiene activos con origen delictivo. Este control

⁸⁴ Álvarez González, J. (2019). *Blanqueo de capitales: cinco parámetros de reducción teleológica a la luz de la jurisprudencia del Tribunal Supremo* [Tesis doctoral, Universidad Complutense de Madrid]. Facultad de Derecho, Universidad Complutense de Madrid.

⁸⁵ Peña Bernaldo de Quirós, M. (1999). *Derechos Reales. Derecho Hipotecario*. Madrid: CRPME.

se ejerce mediante la custodia de claves privadas, lo que permite operar los fondos sin necesidad de formalizar titularidades legales.

- **Utilizar:** El verbo “utilizar”, también previsto expresamente en el tipo penal del artículo 301.1 CP, remite a un comportamiento distinto: el aprovechamiento efectivo del bien, con independencia de que el sujeto sea su propietario o poseedor. Desde una perspectiva civilista, el uso —al que se equipara jurídicamente la utilización— está regulado en el artículo 524 del Código Civil como el derecho a percibir los frutos de una cosa ajena en la medida necesaria para las necesidades del usuario. Como aclaró el Tribunal Supremo en su sentencia de 6 de marzo de 1965, el uso implica un derecho real limitado de goce sobre el bien, orientado a obtener un beneficio concreto o un rendimiento de su explotación.⁸⁶

Trasladado al ámbito penal, utilizar un bien de procedencia ilícita supone realizar con él actos que implican su integración práctica en la esfera de actuación del sujeto activo: financiar actividades, realizar compras, disfrutar de servicios o simplemente obtener un beneficio derivado del bien. A diferencia de la posesión, donde basta con el control fáctico del objeto, en el caso de la utilización se exige una acción positiva de aprovechamiento o explotación del bien, aun cuando esta sea ocasional o transitoria.

La utilización se concreta en el uso de criptoactivos para realizar pagos, financiar servicios, adquirir bienes o facilitar nuevas operaciones delictivas. En este contexto, basta con emplear criptomonedas en la vida económica cotidiana para que el acto resulte penalmente relevante si se conoce su origen ilícito.

- **Convertir:** Este verbo remite a la transformación del bien de modo que su apariencia se desvincule del origen ilícito. Es la forma más característica del blanqueo, e incluye operaciones como el fraccionamiento de dinero para sortear controles bancarios, el uso de testaferros, la adquisición de activos financieros o bienes de lujo, y otras maniobras destinadas a dar apariencia de legalidad al capital delictivo. Lo esencial es que el resultado sea parcial o totalmente distinto del bien originario.

Las operaciones de conversión son particularmente frecuentes en el ecosistema cripto: el canje de monedas ilícitas por stablecoins, el paso por mezcladores (mixers), o la conversión entre tokens en plataformas descentralizadas constituyen supuestos claros de transformación que dificultan la trazabilidad del capital.

- **Transmitir:** Alude al traspaso del bien de una persona a otra, conservando su identidad económica. Aunque desde una perspectiva civil se ha entendido

⁸⁶ Tribunal Supremo, Sala Primera. (1965). *Sentencia de 6 de marzo* (RJ 1965/1124).

tradicionalmente como la cesión jurídica de derechos subjetivos,⁸⁷ en el ámbito penal debe acogerse una interpretación más amplia y funcional, que incluya cualquier forma de desplazamiento patrimonial relevante, incluso si no se formaliza jurídicamente. Como advierte Del Carpio Delgado, una concepción excesivamente restrictiva dejaría fuera supuestos frecuentes de blanqueo en los que se produce una transmisión fáctica de los bienes sin cesión real de derechos.⁸⁸

La transmisión en el contexto cripto puede realizarse mediante simples operaciones de blockchain entre direcciones, sin necesidad de mediación institucional. Esta facilidad técnica permite desplazar grandes cantidades de valor de forma inmediata, anónima y transnacional, encajando plenamente en el verbo típico.

- **Realizar “cualquier otro acto”:** Esta cláusula ha sido objeto de un intenso debate doctrinal debido a su redacción abierta y a las implicaciones que conlleva desde la perspectiva del principio de legalidad. La inclusión de fórmulas de este tipo responde a una técnica legislativa que persigue garantizar la eficacia del tipo penal ante nuevas formas de criminalidad que escapan a los moldes clásicos de comportamiento delictivo. Se trata de ofrecer una respuesta normativa frente a conductas que, si bien no fueron imaginadas por el legislador, satisfacen sustancialmente los fines típicos del precepto.

Parte de la doctrina, interpreta que esta cláusula no hace sino confirmar la naturaleza dinámica del delito de blanqueo. A su juicio, lo que el legislador ha querido reflejar es que el blanqueo no se agota en un acto único, sino que constituye un proceso integrado por diversas fases: colocación, conversión e integración.⁸⁹ Cada una de estas etapas implica actos diversos, muchos de los cuales no se corresponden estrictamente con adquirir, convertir o transmitir, pero que son materialmente aptos para facilitar la legalización del dinero ilícito.

No obstante, esta interpretación funcionalista no está exenta de tensiones. El problema central radica en determinar si esa amplitud permite incluir cualquier conducta con un vínculo remoto o indirecto con los bienes ilícitos. Frente a esta opción, una línea doctrinal y jurisprudencial más restrictiva sostiene que sólo deben considerarse típicas aquellas acciones que, sin coincidir literalmente con los verbos del tipo, sean sustancialmente equivalentes en su capacidad para encubrir o integrar el bien delictivo. Así lo refleja la STS 265/2015, que señala que la finalidad de ocultar o ayudar a eludir

⁸⁷ Lacruz Berdejo, J. L., Luna Serrano, A., & Rivero Hernández, F. (2005). *Elementos de Derecho civil*, tomo I, vol. 3. Madrid: Thomson-Civitas, p. 101.

⁸⁸ Del Carpio Delgado, *op. cit.*, pp. 182–183.

⁸⁹ Existen diversos modelos doctrinales sobre las fases del blanqueo, pero puede seguirse el esquema funcional del GAFI, asumido también por la STS 156/2011, de 21 de marzo, que distingue tres etapas: colocación, estratificación y reintegración.

consecuencias legales constituye un elemento esencial que debe estar presente en cualquier conducta subsumible bajo el art. 301.1 CP.⁹⁰

Por el contrario, otras resoluciones como la STS 457/2007 han defendido una interpretación más abierta, subrayando que la redacción del precepto permite incluir cualquier acto que, aun sin equivaler a adquisición, conversión o transmisión, lesione el bien jurídico protegido: la integridad del orden económico y la transparencia del sistema financiero.⁹¹ No obstante, esta línea interpretativa ha sido objeto de crítica por parte de autores como Del Carpio Delgado, quien advierte que expresiones como “cualquier otro acto” introduce un elevado grado de indeterminación normativa en el tipo penal, lo que, en su opinión, puede resultar incompatible con el principio de legalidad con su exigencia de taxatividad. A su juicio, esta expresión configura una verdadera “cláusula abierta”, que amplía de forma excesiva el alcance del precepto y pone en riesgo las garantías constitucionales propias del Derecho pena.⁹²

A la luz de este debate, puede concluirse que el contenido de esta cláusula requiere una aplicación prudente y ajustada a los principios fundamentales del Derecho penal. En cualquier caso, el debate doctrinal en torno a la amplitud de la cláusula “cualquier otro acto” adquiere una especial relevancia en el contexto del blanqueo de capitales mediante criptoactivos. Su formulación abierta no solo permitiría, sino que incluso facilitaría la subsunción de estas nuevas formas de criminalidad económica, caracterizadas por operaciones tecnológicamente complejas y que difícilmente encajan en las categorías tradicionales de adquisición, conversión o transmisión. Así, pese a las objeciones que esta redacción puede suscitar desde la perspectiva del principio de taxatividad, lo cierto es que ofrece un marco jurídico más flexible y adaptable para hacer frente a fenómenos delictivos emergentes vinculados al uso de tecnologías descentralizadas.

Como puede observarse, las conductas previstas en el artículo 301 CP, adquirir, poseer, utilizar, convertir y transmitir bienes, son perfectamente aplicables a las operaciones con criptomonedas, a pesar de la novedad técnica que estas presentan. Por tanto, puede afirmarse que las conductas típicas recogidas en el artículo 301 CP no requieren una reforma para abarcar las operaciones con criptoactivos, sino una interpretación funcional y tecnológicamente informada. Las particularidades técnicas del ecosistema blockchain, descentralización, pseudonimato, inmediatez, no desnaturalizan el tipo penal, sino que reformulan la forma en que este debe ser aplicado, lo que exige una aplicación del tipo penal que tenga en cuenta la especificidad técnica de estas nuevas formas de actuación delictiva.

c. Elemento finalista:

⁹⁰ Tribunal Supremo, Sala de lo Penal. (2015). *Sentencia 265/2015, de 29 de abril*, FJ 9.^º

⁹¹ Tribunal Supremo, Sala de lo Penal. (2007). *Sentencia 457/2007, de 29 de mayo*, Fundamento Jurídico 3.^º

⁹² Del Carpio Delgado, *op. cit.*, pp. 182–183.

Uno de los aspectos definatorios del delito de blanqueo de capitales es su carácter de delito de tendencia interna trascendente⁹³, lo que significa que la conducta típica debe ir dirigida a una finalidad concreta para ser penalmente relevante. El artículo 301.1 CP exige que los actos sobre bienes de origen delictivo —como adquirir, poseer, utilizar, convertir, transmitir o realizar cualquier otro acto— tengan como objetivo: ocultar o encubrir su origen ilícito, o ayudar a los partícipes del delito antecedente a eludir las consecuencias legales de sus actos.

Respecto a la primera finalidad, el propio precepto alude expresamente al "encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes", lo que evidencia que se castiga cualquier acción idónea para dificultar la trazabilidad del capital delictivo.

La segunda finalidad, de eludir las consecuencias legales, se refiere a comportamientos orientados a evitar la detección, persecución o decomiso de los bienes ilícitos, permitiendo su disfrute por el autor o por terceros.

En todo caso, no se requiere que el resultado se materialice, sino que basta con que la conducta esté objetivamente dirigida a alguno de los fines típicos. Así, se configura una finalidad objetiva del acto, inferible del contexto, sin necesidad de probar un dolo específico o un propósito subjetivo más allá del conocimiento del origen delictivo.⁹⁴

d. Tipicidad subjetiva: dolo e imprudencia.

La tipicidad subjetiva en el delito de blanqueo de capitales puede revestir dos formas principales: el dolo directo o eventual, como modalidad típica y predominante, y la imprudencia grave, cuya inclusión expresa en el artículo 301.3 del Código Penal reviste particular relevancia en el ámbito de las personas jurídicas y los sujetos obligados por la legislación preventiva. Esta doble vía de imputación responde al carácter plural del bien jurídico protegido y a la necesidad de abarcar tanto las conductas deliberadas como aquellas basadas en una omisión grave del deber de prevención, especialmente cuando quien actúa tiene capacidad profesional o estructural para detectar operaciones irregulares. En el contexto de los criptoactivos, esta configuración cobra especial sentido, dada la opacidad tecnológica que rodea muchas de estas operaciones y la creciente obligación de quienes operan en este entorno de adoptar medidas técnicas y organizativas eficaces.

- **Dolo**

El tipo penal del artículo 301 CP exige normalmente que el autor conozca el origen delictivo de los bienes y actúe con la intención de ocultarlo, encubrirlo o facilitar que se eludan las consecuencias jurídicas del delito fuente. No obstante, la jurisprudencia del Tribunal Supremo ha rebajado el umbral de exigencia probatoria, señalando que no se requiere una identificación exacta del delito precedente, sino que basta con que el sujeto actúe con conciencia de la anormalidad de la operación o del probable origen ilícito del bien⁹⁵. Este estándar

⁹³ Mir Puig, S. (2020). *Derecho penal. Parte general* (11.ª ed.). Barcelona: Reppertor Jurídico, p. 152.

⁹⁴ Blanco Cordero, *op. cit.*

⁹⁵ STS 2410/2001 y STS 1637/2000, *op. cit.*

de dolo eventual, reconocido en la STS 2410/2001 y consolidado en la STS 1637/2000, permite sancionar aquellas conductas en las que, sin tener certeza plena, el autor acepta el riesgo de colaborar en la integración de bienes de origen criminal.

- **Imprudencia grave**

La introducción de la imprudencia grave como modalidad punible del delito de blanqueo responde a la necesidad de perseguir conductas en las que no exista dolo, pero sí una omisión grave de los deberes de control exigibles a determinados sujetos por su posición en el sistema económico. Esta previsión cobra especial relevancia en el caso de las personas jurídicas, especialmente entidades financieras y operadores de servicios sobre criptoactivos, que están sometidos a estrictas obligaciones de prevención conforme a la Ley 10/2010, al Reglamento AML de 2024 y a la Directiva (UE) 2018/1673.⁹⁶

La doctrina ha señalado que el blanqueo imprudente requiere que el sujeto omita el deber de actuar ante señales objetivas que habrían permitido identificar la operación como sospechosa. Esta modalidad se justifica en el incumplimiento grave de la obligación de vigilancia, no en una intención encubridora.⁹⁷ Por ello, su aplicación práctica se ha concentrado en profesionales del sector financiero, sujetos obligados y, en los últimos años, empresas de servicios sobre criptoactivos, como exchanges, custodios y plataformas de compraventa⁹⁸.

La jurisprudencia también ha matizado que esta forma de imputación no puede extenderse de forma automática a cualquier descuido, pues ello vulneraría el principio de intervención mínima. En la STS 924/2005, se rechaza una interpretación expansiva de la imprudencia que lleve a sancionar situaciones de riesgo abstracto, sin prueba suficiente de la omisión relevante.⁹⁹ En consecuencia, solo puede apreciarse responsabilidad imprudente cuando exista una negligencia cualificada, es decir, una infracción clara de los estándares de diligencia exigibles al operador.

Este enfoque cobra especial importancia en el ámbito de los criptoactivos, donde las estructuras descentralizadas, la pseudonimidad de los usuarios y la volatilidad de la regulación dificultan el cumplimiento de las obligaciones tradicionales de vigilancia. Sin embargo, esto no exime de responsabilidad: el Reglamento AML y la regulación MiCA ya exigen que las plataformas de intercambio apliquen medidas efectivas de identificación del cliente (KYC), análisis de operaciones sospechosas (AML) y control de fondos. La omisión sistemática o negligente de estas obligaciones podría ser constitutiva de imprudencia penal grave, especialmente si la empresa no implementa protocolos internos de detección y respuesta adecuados¹⁰⁰.

⁹⁶ Directiva (UE) 2018/1673, art. 3.4 y 5; Reglamento (UE) 2024/1624, arts. 3 y 9.

⁹⁷ Nieto Martín, A. (2019). *Responsabilidad penal de la persona jurídica*. Tirant lo Blanch.

⁹⁸ ¹ FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

⁹⁹ STS 924/2005, de 17 de junio, FJ 4.º.

¹⁰⁰ EBA & ESMA. (2025). *Joint Report on recent developments in crypto-assets*. Brussels: EU Publications.

En definitiva, la imprudencia en el blanqueo no debe entenderse como una simple negligencia ocasional, sino como una omisión estructural de deberes de control y prevención, especialmente cuando la persona jurídica dispone de los medios técnicos y humanos para detectar riesgos operativos, pero elige no activarlos.

3.3.3. Fases tradicionales del blanqueo y su ejecución con criptoactivos

Tradicionalmente, el delito de blanqueo de capitales se estructura en tres fases: colocación, estratificación (también denominada *layering*) e integración. En la primera, se introduce el dinero ilícito en el sistema económico, normalmente mediante su depósito fraccionado en instituciones financieras. La segunda implica una cadena de transacciones que busca dificultar el rastro del origen, mientras que en la tercera se reinvierte el dinero con apariencia de licitud en actividades legales.¹⁰¹

Los criptoactivos se han incorporado a estas fases como herramientas funcionales que multiplican las posibilidades del blanqueo. Durante la colocación, permiten la entrada de fondos sin necesidad de intermediarios financieros tradicionales, gracias a su estructura descentralizada. En la fase de estratificación, se utilizan diversos instrumentos digitales que rompen la conexión directa entre el emisor y el receptor de los fondos. Entre ellos destacan:

- Los mixers o tumblers, que son servicios diseñados para mezclar criptomonedas procedentes de múltiples usuarios, generando una cadena de transacciones que oculta su origen exacto y dificulta la trazabilidad.¹⁰²
- Las plataformas peer-to-peer (P2P), que permiten intercambios directos entre personas sin pasar por plataformas centralizadas, eludiendo los controles de identidad tradicionales.¹⁰³
- Las wallets frías, que son monederos digitales sin conexión a internet (como dispositivos físicos o almacenamiento en papel), empleados para ocultar fondos y desconectarlos del circuito financiero rastreable.¹⁰⁴

En la etapa final, la integración, los activos digitales se reconvierten en bienes aparentemente lícitos, como inmuebles, vehículos o incluso arte digital (NFTs), a través de exchanges regulados o redes de compraventa privadas (over-the-counter, OTC)¹⁰⁵. De esta forma, las criptomonedas pasan a formar parte del tráfico económico legal con una apariencia de legitimidad.

Este conjunto de mecanismos, como advierte el Parlamento Europeo, ha motivado una creciente preocupación por la vinculación entre el uso de criptomonedas y actividades

¹⁰¹ STS 156/2011, de 21 de marzo, FJ 3.º

¹⁰² Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European Union Agency for Law Enforcement Cooperation.

¹⁰³ GAFI-FATF. (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. París: Financial Action Task Force.

¹⁰⁴ Parlamento Europeo (2020). Op. Cit.

¹⁰⁵ BBVA, *¿Qué son los mercados over the counter (OTC)?*, 2021. Disponible en: <https://www.bbva.com/es/que-son-los-mercados-over-the-counter-otc/> [última consulta: 8 de mayo de 2025].

delictivas, especialmente el blanqueo de capitales. En su Resolución de 2020, el Parlamento subrayó que una parte significativa de las operaciones con criptoactivos puede estar asociada a delitos, instando a reforzar los marcos regulatorios y supervisores.¹⁰⁶

En definitiva, el artículo 301 del Código Penal configura un tipo penal amplio, dinámico y funcionalmente adaptado a las complejidades del delito de blanqueo de capitales, incluso en su dimensión digital. La jurisprudencia y la doctrina han contribuido a perfilar sus elementos con criterios que buscan conjugar la efectividad de la persecución penal con las garantías del Derecho penal moderno. Sin embargo, la creciente sofisticación de los métodos empleados, especialmente mediante el uso de criptoactivos, pone de relieve los límites del enfoque exclusivamente represivo, reforzando la necesidad de medidas preventivas. Es en este contexto donde cobra pleno sentido el análisis de la regulación administrativa del blanqueo, orientada a anticiparse al riesgo mediante obligaciones de control, identificación y reporte.

3.4. Regulación administrativa

3.4.1. Normativa europea:

La lucha contra el blanqueo de capitales y la financiación del terrorismo constituye una prioridad en la política legislativa de la Unión Europea (UE), especialmente desde la década de los noventa. A lo largo de estas décadas, la UE onstruido un marco jurídico cada vez más sofisticado, centrado inicialmente en el ámbito financiero, pero que ha ido expandiéndose hacia sectores no financieros y, más recientemente, hacia entornos tecnológicos emergentes como el de los criptoactivos. Este sistema normativo se ha desarrollado en estrecha sintonía con las Cuarenta Recomendaciones del Grupo de Acción Financiera Internacional (GAFI), entidad intergubernamental creada en 1989 en París por iniciativa de los países miembros del G7 y que actualmente está integrado por 37 jurisdicciones.¹⁰⁷ Si bien dichas recomendaciones carecen de fuerza jurídica vinculante, operan como verdaderas normas de soft law y constituyen el estándar internacional en la materia.¹⁰⁸

Este cuerpo normativo se inició con la Primera Directiva 91/308/CEE,¹⁰⁹ centrada en el ámbito financiero, y se consolida con la Cuarta Directiva (UE) 2015/849 y la Quinta Directiva (UE) 2018/843, que introducen instrumentos estructurales esenciales como el enfoque basado en el riesgo, los registros de titularidad real, la diligencia debida

¹⁰⁶ Parlamento Europeo (2020), op. cit

¹⁰⁷ Blanco Cordero, I., Fabián Caparrós, E., Prado Saldarriaga, V., Santander Abril, G. & Zaragoza Aguado, J. *Combate al lavado de activos desde el sistema judicial*, OEA, 2018, pp. 136-143

¹⁰⁸ Véase Díaz-Maroto y Villarejo, J. (2017). *El lavado de activos o blanqueo de capitales y su regulación en España*. Revista Peruana de Ciencias Penales, (31), 133–170.
<https://doi.org/10.31381/rpcp.v0i31.1435>, Grupo de Acción Financiera Internacional (GAFI). (2012). *Las 40 recomendaciones del GAFI*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/Recommendations/FATF-40-Rec-2012-Spanish.pdf>

¹⁰⁹ Directiva 91/308/CEE, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales. *Diario Oficial de las Comunidades Europeas*, L 166, de 28 de junio de 1991. ELI: <https://eur-lex.europa.eu/legal-content/ES/ELI/DIR/1991/308/oj>

reforzada, la ampliación del elenco de sujetos obligados, y la incorporación de operadores vinculados a los criptoactivos. A este marco preventivo se suma la Sexta Directiva (UE) 2018/1673, que armoniza, por primera vez, los elementos típicos y las sanciones penales asociadas al delito de blanqueo de capitales en los Estados miembros, configurando así un sistema mixto de prevención y represión.¹¹⁰

En conjunto, estas directivas han establecido los principios fundamentales del sistema europeo, un sistema que se articula mediante un modelo de prevención basado en la colaboración obligatoria del sector privado, imponiendo obligaciones normativas directas a determinados operadores económicos y profesionales, dotándolos de un papel central en la detección temprana de operaciones de blanqueo. Su transposición al ordenamiento español se ha materializado, fundamentalmente, a través de la Ley 10/2010¹¹¹, que constituye el pilar del régimen preventivo nacional.

Ahora bien, la irrupción de los criptoactivos y su creciente utilización en operaciones tanto legítimas como ilícitas ha generado nuevos desafíos jurídicos. La ausencia de normas armonizadas específicas para este sector generaba vacíos normativos que ponían en riesgo la eficacia del sistema europeo de prevención. Como respuesta a esta carencia, la Unión Europea aprobó el Reglamento (UE) 2023/1114, conocido como MiCA (Markets in Crypto-Assets),¹¹² que establece por primera vez un marco jurídico común para los emisores y proveedores de servicios de criptoactivos en toda la UE. Aunque MiCA regula aspectos estructurales del mercado cripto, proporciona las condiciones normativas necesarias para la integración del sector cripto en el régimen de cumplimiento y supervisión regulatoria.

Esta iniciativa forma parte del denominado AML Package, presentado por la Comisión Europea en julio de 2021¹¹³, cuyo objetivo es reforzar de forma coherente el sistema europeo de prevención del blanqueo de capitales. Este paquete legislativo se completa con tres nuevos instrumentos adoptados en mayo de 2024. En primer lugar, el Reglamento (UE) 2024/1624 (AML), que por primera vez establece un marco único y directamente aplicable de prevención del blanqueo de capitales y financiación del terrorismo en la UE. Esta norma amplía el catálogo de sujetos obligados a sectores como los CASPs (Crypto-Asset Service Providers), entre otros. En segundo lugar, el Reglamento (UE) 2024/1620, que crea la nueva Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo (ALBC), con sede en Fráncfort, y que asumirá funciones de supervisión directa e indirecta sobre entidades de alto riesgo. Y finalmente, la Directiva (UE)

¹¹⁰ Directiva (UE) 2018/1673, de 23 de octubre de 2018, sobre la lucha contra el blanqueo de capitales mediante el Derecho penal. *Diario Oficial de la Unión Europea*, L 284, de 12 de noviembre de 2018. ELI: <https://eur-lex.europa.eu/legal-content/ES/ELI/DIR/2018/1673/oj>

¹¹¹ Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado*, 103, de 29 de abril de 2010. ELI: <https://www.boe.es/eli/es/l/2010/04/28/10>

¹¹² Reglamento (UE) 2023/1114, de 31 de mayo de 2023, sobre los mercados de criptoactivos. *Diario Oficial de la Unión Europea*, L 150, de 9 de junio de 2023. ELI: <https://eur-lex.europa.eu/legal-content/ES/ELI/REG/2023/1114/oj>

¹¹³ Consejo de la Unión Europea. (2024, 30 de mayo). *Lucha contra el blanqueo de capitales: el Consejo adopta un paquete de normas*. [Nota de prensa]. <https://www.consilium.europa.eu/es/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>

2024/1640, centrada en reforzar la organización y coordinación de las autoridades nacionales competentes, especialmente las UIF y los supervisores.

Por tanto, la regulación europea en esta materia se estructura actualmente en torno a dos grandes pilares complementarios: por un lado, las directivas y normas administrativas ya consolidadas, que han dado forma a un modelo preventivo robusto; por otro, los nuevos reglamentos con efecto directo, que armonizan el tratamiento jurídico del riesgo de blanqueo en sectores emergentes, especialmente en el entorno digital. En este contexto, el análisis de MiCA y del nuevo Reglamento AML resulta esencial para valorar la adecuación del marco normativo europeo frente a los desafíos que plantea el uso del ecosistema cripto en esquemas de criminalidad económica compleja.

a. Los mecanismos de prevención en la regulación europea: principales medidas

El sistema europeo de prevención del blanqueo se ha construido mediante un proceso legislativo gradual, caracterizado por la incorporación progresiva de medidas técnicas y jurídicas destinadas a evitar la introducción y circulación de fondos ilícitos en el circuito financiero legal. A continuación, se exponen los mecanismos fundamentales, cuya combinación articula el núcleo del modelo preventivo.

En primer lugar, la obligación de identificación del cliente (KYC) y la aplicación de medidas de diligencia debida (DDC)¹¹⁴, introducida ya en la Primera Directiva y sistematizada en la Tercera (2005/60/CE) y Cuarta Directiva (2015/849), exige a las entidades verificar la identidad de sus clientes antes de iniciar relaciones de negocio. Este deber incluye la adaptación del nivel de control en función del riesgo asociado a la operación, conforme al principio de proporcionalidad, y requiere prestar atención reforzada sobre aquellas transacciones que, por su naturaleza o cuantía, puedan vincularse al blanqueo de capitales.

En segundo lugar, la creación de registros de titularidad real¹¹⁵, establecida por la Cuarta Directiva y reforzada por la Quinta (2018/843), ha permitido avanzar en la desarticulación de estructuras jurídicas opacas. Esta medida obliga a los Estados miembros a establecer registros nacionales, interconectados a escala europea y con acceso público parcial, que permitan identificar a las personas físicas que, directa o indirectamente, controlan entidades jurídicas. Con ello se dificulta el uso instrumental de sociedades pantalla, fideicomisos u otras figuras jurídicas con finalidades de encubrimiento patrimonial.

En tercer lugar, el deber de comunicación de operaciones sospechosas¹¹⁶ se ha consolidado como uno de los pilares del sistema. Desde la Primera Directiva, los sujetos obligados deben informar a las Unidades de Inteligencia Financiera (FIUs)¹¹⁷ de cualquier

¹¹⁴ 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, arts. 17 a 30.

¹¹⁵ Reglamento (UE) 2024/1624, arts. 44 a 48.

¹¹⁶ Reglamento (UE) 2024/1624, arts. 50 a 56.

¹¹⁷ Las Unidades de Inteligencia Financiera (FIUs, por sus siglas en inglés) son organismos nacionales encargados de recibir, analizar y comunicar información sobre operaciones financieras sospechosas vinculadas al blanqueo de capitales y la financiación del terrorismo. En España, esta función la

operación que, por su forma, cuantía, frecuencia o características inusuales, despierte indicios de vinculación con el blanqueo o la financiación del terrorismo. Este mecanismo representa una manifestación de la cooperación público-privada, y ha sido identificado como un instrumento esencial para la detección anticipada de esquemas complejos de ocultación.

En cuarto lugar, las entidades sujetas al régimen preventivo deben conservar toda la documentación¹¹⁸ relativa a la identificación del cliente, operaciones y comunicaciones durante un plazo mínimo de cinco años. Esta obligación, prevista inicialmente en la Cuarta Directiva y hoy consolidada en el Reglamento AML, permite garantizar la trazabilidad posterior de los fondos y facilita la reconstrucción ex post por parte de las autoridades administrativas y judiciales de operaciones complejas o disimuladas, especialmente en contextos digitales donde la volatilidad y rapidez de las transacciones podría dificultar el control retrospectivo.

En quinto lugar, debe destacarse la ampliación progresiva del ámbito subjetivo del régimen preventivo¹¹⁹ obligados dentro del marco preventivo europeo. Mientras que las primeras directivas se limitaban al sector financiero, la Segunda Directiva (2001/97/CE) extendió por primera vez estas obligaciones a profesionales no financieros, como abogados, notarios o agentes inmobiliarios. Este proceso continuó con la Quinta Directiva (UE) 2018/843, que, por primera vez, incluyó expresamente a los proveedores de servicios de cambio de criptomonedas por moneda fiduciaria y de custodia de monederos electrónicos, reconociendo así los nuevos riesgos derivados del ecosistema cripto. Sin embargo, aquella regulación tenía un alcance limitado y requería transposición nacional. Será el Reglamento AML el que establezca, por primera vez, una obligación directa y uniforme para todos los proveedores de servicios sobre criptoactivos (CASPs) en la Unión Europea, consolidando así un marco de supervisión coordinado, en consonancia con la definición y regulación de estos operadores contenida en el Reglamento MiCA.

Finalmente, la normativa europea impone a los sujetos obligados la implementación de políticas, procedimientos y mecanismos internos (obligación de compliance)¹²⁰ adecuados para la gestión eficaz del riesgo de blanqueo de capitales y financiación del terrorismo. Esta exigencia incluye, entre otros aspectos, la designación de un responsable de cumplimiento normativo, la adopción de protocolos de detección y reporte, la formación continua del personal, y la auditoría interna periódica. Estas obligaciones, ya presentes en la Cuarta, han sido reforzadas por el Reglamento AML, donde se detallan los requisitos mínimos de gobernanza interna. Su finalidad es asegurar que los sujetos obligados no solo cumplan formalmente con los deberes de información, sino que desarrollen una cultura de cumplimiento estructural, capaz de detectar y mitigar proactivamente ante riesgos emergentes, especialmente en entornos tecnológicos como el de los criptoactivos.

desempeña el SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias). Véase GAFI (2023), *Revisión de la función de las FIUs*, disponible en: <https://www.fatf-gafi.org/>.

¹¹⁸ Reglamento (UE) 2024/1624, arts. 31 y 32.

¹¹⁹ Reglamento (UE) 2024/1624, art. 3.

¹²⁰ Reglamento (UE) 2024/1624, art. 3.

A pesar de su solidez normativa, los mecanismos tradicionales de prevención presentan importantes limitaciones cuando se aplican al ecosistema de los criptoactivos. En particular, la efectividad de las medidas de identificación del cliente (KYC) se ve comprometida en el entorno cripto cuando las operaciones se realizan a través de plataformas descentralizadas (DEX), redes peer-to-peer o monederos no custodiados. En estos casos, al no existir intermediarios sujetos a regulación ni responsables de verificar la identidad del usuario, resulta inviable aplicar los mecanismos tradicionales de control. Del mismo modo, el deber de comunicación de operaciones sospechosas pierde eficacia cuando las transacciones se realizan fuera del circuito financiero formal, como ocurre en intercambios P2P o a través de wallets autónomas. En cuanto a los registros de titularidad real, su utilidad se reduce en la medida en que muchas estructuras cripto permiten ocultar la identidad del beneficiario final mediante capas técnicas. Por el contrario, medidas como la conservación documental o la implementación de políticas internas de compliance sí pueden resultar efectivas, siempre que los proveedores de servicios sobre criptoactivos estén sometidos a regulación y supervisión efectiva. En conjunto, la adaptación del marco preventivo europeo al entorno digital exige no solo extender las obligaciones legales a los nuevos operadores, sino también garantizar la viabilidad técnica y operativa de su cumplimiento.

3.4.2. el Reglamento MiCA

El Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (*Markets in Crypto-Assets*, MiCA), forma parte del denominado *AML Package* propuesto por la Comisión Europea en 2021¹²¹, y constituye el primer marco jurídico armonizado a nivel europeo específicamente destinado a regular la emisión, oferta pública y prestación de servicios sobre criptoactivos no cubiertos por las normas financieras tradicionales. Su adopción se enmarca en la estrategia de la Unión Europea por integrar los activos digitales dentro del mercado interior, asegurando la protección del inversor, la estabilidad financiera y la integridad del mercado.

Desde la perspectiva del presente trabajo, centrado en la adecuación de la normativa vigente frente al blanqueo de capitales mediante el uso de criptoactivos, la relevancia de MiCA reside en su capacidad para eliminar zonas grises normativas previamente explotadas por operadores no regulados, así como en su función instrumental para facilitar la aplicación coordinada de medidas preventivas previstas en el Reglamento AML. El Reglamento apuesta por un modelo de control preventivo y estructural, basado en la autorización, supervisión y cumplimiento de condiciones ex ante. Esta lógica preventiva contrasta con el enfoque penal ex post tradicional, lo que justifica su coordinación con normas como el futuro Reglamento AML.¹²²

¹²¹ Comisión Europea. (2021, 20 de julio). *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules* [Nota de prensa]. Comisión Europea. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

¹²² Pérez Marín, M. Á. (2023). *El reglamento MiCA: responsabilidad y sanción frente al incumplimiento de la regulación*. *Ius et Scientia*, 9(2), 64–92. <https://doi.org/10.12795/IESTSCIENTIA.2023.i02.04>

a. Objetivos del reglamento MiCA

El Reglamento MiCA persigue tres objetivos fundamentales: i) dotar de seguridad jurídica al mercado de criptoactivos mediante la definición y clasificación de estos instrumentos digitales; ii) fomentar la innovación tecnológica en un entorno normativo homogéneo; y iii) proteger a los consumidores, garantizar la integridad del mercado y preservar la estabilidad financiera.

En cuanto a su ámbito de aplicación, MiCA, en su artículo 2, regula los criptoactivos que no se califican como instrumentos financieros conforme a la Directiva 2014/65/UE (MiFID II),¹²³ y que, por tanto, no están cubiertos por la legislación financiera sectorial. Quedan excluidos expresamente los tokens no fungibles no fraccionables (NFTs), las monedas digitales emitidas por bancos centrales (CBDCs) y los tokens de uso exclusivamente limitado (las que solo pueden canjearse dentro de un entorno cerrado, por ejemplo, puntos de fidelización en comercios o plataformas cerradas).¹²⁴

Por tanto, el Reglamento se aplica fundamentalmente a tres tipos de criptoactivos, tal y como se definen en el artículo 3:

- Tokens de utilidad (utility tokens), que permiten acceder a un bien o servicio digital proporcionado por el emisor (por ejemplo, acceso anticipado a una plataforma o aplicación).
- Tokens referenciados a activos (asset-referenced tokens, ART), cuyo valor se mantiene estable por estar vinculado a una cesta de activos (divisas, materias primas, otros criptoactivos).
- Tokens de dinero electrónico (e-money tokens, EMT), que tienen por objeto actuar como medio de pago, manteniendo su valor referenciado a una única moneda oficial (como el euro o el dólar).

Esta clasificación es crucial para el presente trabajo, ya que fija los parámetros sobre los cuales se articula el control regulatorio y la posible intervención de las autoridades administrativas y financieras para prevenir el uso de estos instrumentos en esquemas de blanqueo de capitales

b. Proveedores de servicios sobre criptoactivos (CASps)

Una de las principales aportaciones del Reglamento MiCA reside en la creación de una categoría jurídica específica: los Proveedores de Servicios sobre Criptoactivos (CASPs).

¹²³ La Directiva 2014/65/UE, conocida como MiFID II (*Markets in Financial Instruments Directive*), es la norma europea que regula la prestación de servicios de inversión y el funcionamiento de los mercados financieros en la Unión Europea. Su objetivo principal es reforzar la transparencia, integridad y protección del inversor, estableciendo criterios para la clasificación de instrumentos financieros, incluidos aquellos tokenizados, que quedan fuera del ámbito de aplicación del Reglamento MiCA.

¹²⁴ Parlamento Europeo. (2020). *Crypto-assets: Key developments, regulatory concerns and responses*. PE 648.779.

Esta figura agrupa a las plataformas de intercambio, custodios, emisores y otras entidades que prestan servicios de asesoramiento, ejecución, colocación o gestión de carteras de criptoactivos.

Conforme al artículo 53 del Reglamento, estos operadores deben constituirse como personas jurídicas con sede en la Unión Europea y obtener autorización previa de la autoridad nacional competente —en España, la CNMV—. La autorización requiere el cumplimiento de requisitos de solvencia, honorabilidad, organización interna, ciberseguridad y gestión de conflictos de interés (arts. 59 a 67).

Además, los emisores deben redactar un White Paper o documento informativo, regulado en los artículos 5 a 15, que incluya información técnica y jurídica sobre los criptoactivos ofertados, los riesgos inherentes, las condiciones de la emisión, los derechos de los tenedores y advertencias sobre la ausencia de garantías institucionales. Esta obligación de transparencia constituye una herramienta clave para combatir la opacidad y prevenir el uso fraudulento de estos activos.¹²⁵

c. Obligaciones relevantes de MiCA en relación con la prevención del blanqueo de capitales

Aunque el Reglamento MiCa no es una norma de naturaleza penal, sí establece un conjunto de obligaciones jurídicas preventivas de carácter administrativo, cuyo incumplimiento puede dar lugar a sanciones económicas y correctivas, sin que ello implique per se la atribución de responsabilidad penal directa, salvo en los casos en los que los hechos puedan dar lugar a la intervención de la jurisdicción penal, conforme a lo previsto en sus artículos 124 y 125.¹²⁶ Estas obligaciones permiten la identificación, regulación y supervisión de los actores que intervienen en el ecosistema cripto, lo cual resulta esencial para la prevención del blanqueo.

En primer lugar, el artículo 53 del Reglamento MiCA permite la construcción de un registro de operadores legítimos, lo que facilita su integración como sujetos obligados en el Reglamento AML.¹²⁷

A continuación, el Reglamento impone en su Título V (arts. 59 a 67) un conjunto de requisitos de organización interna, solvencia y gobernanza. Los CASPs deben contar con estructuras administrativas adecuadas, mantener fondos propios suficientes, garantizar la honorabilidad e idoneidad profesional de sus órganos de dirección, y disponer de sistemas eficaces de gestión de riesgos, auditoría interna y prevención de conflictos de interés. Estos elementos son esenciales para garantizar un funcionamiento transparente, fiable y conforme a estándares éticos mínimos.¹²⁸

De especial importancia en clave de prevención es la regulación de la custodia de criptoactivos. El artículo 67 impone a los CASPs la obligación de mantener los

¹²⁵ Parrondo, L., *op. cit.*, pp. 15–16.

¹²⁶ Pérez Marín, *op. cit.*

¹²⁷ Parrondo, L. (2023). *El Reglamento de Mercados en Criptoactivos (MiCA)*. Técnica Contable y Financiera, (septiembre), 1–26. UPF Barcelona School of Management

¹²⁸ Comisión Nacional del Mercado de Valores (s.f.). *Regulación de los criptoactivos: Reglamento MiCA*. CNMV. <https://www.cnmv.es/Portal/mica/regulacion-criptoactivos?lang=es>

criptoactivos separados de los fondos de sus clientes, abstenerse de utilizarlos por cuenta propia sin consentimiento expreso y garantizar la disponibilidad de los activos en caso de insolvencia del proveedor, lo que reduce considerablemente el riesgo de apropiación indebida o desaparición patrimonial. Estos mecanismos aseguran la trazabilidad del patrimonio digital y dificultan su desvío con fines ilícitos.¹²⁹

Asimismo, conforme a los artículos 5 a 15 de MiCA, contienen la obligación de redactar el “White Paper”.

Por otro lado, en el ámbito del funcionamiento general de los CASPs, el Reglamento impone obligaciones adicionales de conducta, entre ellas la gestión de conflictos de interés, la información clara, imparcial y no engañosa a los clientes, y la existencia de procedimientos eficaces de resolución de quejas (en los artículos 68 y 69). Estas obligaciones refuerzan la integridad del servicio y contribuyen a detectar posibles operaciones irregulares u opacas que puedan ocultar una finalidad delictiva.

Finalmente, MiCA introduce un régimen específico para los tokens considerados significativos (debido a su potencial impacto sistémico), los ART y EMT. El artículo 43, en coordinación con la supervisión de la Autoridad Bancaria Europea (EBA) y la Autoridad Europea de Valores y Mercados (ESMA),¹³⁰ prevé la aplicación de requisitos adicionales de capital, control operativo y transparencia, en función de criterios como el volumen de transacciones, la cantidad de usuarios o el valor total en circulación. Estas medidas incluyen requisitos reforzados de capital, gobernanza, transparencia y control prudencial, con el objetivo de minimizar su potencial impacto sistémico y su posible instrumentalización en esquemas de blanqueo a gran escala.

En definitiva, el conjunto de obligaciones impuestas por MiCA contribuye a la creación de un marco estructural idóneo para identificar, controlar y sancionar las actividades económicas ilícitas asociadas al uso de criptoactivos. Si bien su aplicación efectiva depende de la coordinación con el Reglamento AML y de la supervisión administrativa, constituye una base jurídica imprescindible para el abordaje preventivo del blanqueo de capitales en el ámbito cripto.

d. Crítica doctrinal sobre los límites del ámbito de aplicación del Reglamento MiCA

A pesar de sus avances, MiCA no regula ni alcanza a todos los instrumentos del mercado cripto. En particular, su exclusión de criptomonedas descentralizadas como Bitcoin, Ether o Monero, cuando no existe un CASP intermediario, limita su eficacia frente a esquemas anónimos y no trazables de blanqueo de capitales¹³¹.

Del mismo modo, la exclusión de los NFTs no fraccionados, pese a su creciente utilización en operaciones especulativas y opacas, deja fuera del ámbito regulador un tipo

¹²⁹ Ibid.

¹³⁰ EBA y ESMA fueron creadas por los Reglamentos (UE) 1093/2010 y 1095/2010, respectivamente, como autoridades supervisoras en el sistema financiero europeo y ejercen funciones específicas en la aplicación del Reglamento MiCA, especialmente respecto de los tokens significativos.

¹³¹ Parrondo, L., *op. cit.*, p. 11.

de activo que puede encubrir valor patrimonial de forma difícilmente detectable por los supervisores.

A ello se suma la ausencia total de regulación sobre las finanzas descentralizadas (DeFi), cuyo funcionamiento mediante smart contracts y sin intermediarios impide aplicar medidas de diligencia debida o reporte. La doctrina ha planteado la necesidad de una futura ampliación del marco legal bajo la denominación provisional de “MiCA 2.0”.¹³²

Además, la ambigüedad respecto de las facultades de inspección y supervisión asignadas a las autoridades nacionales y europeas ha sido objeto de crítica por parte de la doctrina, en la medida en que estas funciones pueden adquirir una dimensión sancionadora que se aproxima a la investigación penal sin las garantías propias del procedimiento penal, lo que plantea tensiones con principios como *nemo tenetur* y *non bis in idem*.¹³³

En conjunto, MiCA representa un avance sin precedentes en la institucionalización del mercado europeo de criptoactivos, y sienta las bases jurídicas necesarias para su integración en el sistema de prevención del blanqueo de capitales. No obstante, la eficacia real del modelo requiere una aplicación coordinada con el Reglamento AML, una interpretación expansiva del concepto de sujeto obligado y un diseño legislativo evolutivo que permita cerrar las brechas detectadas.

3.4.3. *El reglamento AML: consolidación del marco preventivo y apoyo estructural a la persecución penal del blanqueo con criptoactivos*

a. Naturaleza y finalidad del Reglamento AML

Este Reglamento representa un punto de inflexión en la arquitectura normativa comunitaria. Frente al modelo previo, basado exclusivamente en directivas cuya transposición nacional generaba fragmentación y disfunciones, este nuevo instrumento establece un marco jurídico único y directamente aplicable en toda la Unión Europea, con el objetivo de armonizar los estándares mínimos de diligencia, supervisión y control.¹³⁴ Aunque se trata de una norma de naturaleza administrativa, sus disposiciones tienen un impacto directo en la eficacia del sistema represivo penal, al reforzar los mecanismos que permiten detectar, rastrear y probar las operaciones sospechosas realizadas con criptoactivos.

b. Aportaciones relevantes para la prevención y detección penal

Una de las novedades de mayor relevancia es la ampliación del elenco de sujetos obligados al incluir en su artículo 3, de forma expresa y general, a los proveedores de servicios sobre criptoactivos (CASPs) definidos por el Reglamento MiCA. A diferencia del régimen anterior, que solo aludía a los proveedores de cambio de monedas virtuales y custodia de monederos electrónicos, el nuevo Reglamento integra de manera sistemática todo el ecosistema de intermediación cripto, esto es, todas aquellas entidades que prestan servicios vinculados a la emisión, oferta, negociación, transferencia, custodia o asesoramiento sobre criptoactivos, incluyendo exchanges centralizados, proveedores de servicios de staking, plataformas de préstamos con criptoactivos, y otros intermediarios

¹³² Sanz Bayón, P., *op. cit.*, p. 90

¹³³ Pérez Marín, *op. cit.*

¹³⁴ Comisión Europea (2021), *op. cit.*

técnicos o financieros que operen como canalizadores del tráfico económico digital,¹³⁵ imponiendo sobre él obligaciones de diligencia debida, identificación de titularidad real, conservación documental y reporte. Esto permite cerrar brechas normativas que facilitaban el uso de plataformas opacas para el blanqueo de fondos procedentes de actividades ilícitas.

Otra aportación fundamental radica en el fortalecimiento del régimen de identificación del titular real contenido en los artículos del 51 al 56, especialmente en estructuras empresariales complejas o de carácter transnacional. La norma introduce definiciones más detalladas y criterios unificados sobre qué debe entenderse por control efectivo, así como mecanismos para inscripción obligatoria en registros centralizados, lo cual facilita el acceso de las autoridades a información clave para reconstruir el rastro patrimonial en procesos penales.

El Reglamento también establece, por primera vez, en sus artículos 9 y 10 un sistema estandarizado de gobernanza interna aplicable a todos los sujetos obligados, con la obligación de designar tanto un AML Manager —miembro del órgano de administración responsable de supervisar el cumplimiento normativo a alto nivel— como un AML Officer, encargado de la implementación operativa y de actuar como punto de contacto con las autoridades competentes¹³⁶. Esta estructura organizativa, inspirada en las Directrices de la Autoridad Bancaria Europea (2022), refuerza la trazabilidad institucional de las decisiones y responsabilidades, lo que puede resultar especialmente relevante en procesos penales por blanqueo cometido a través de entidades formalmente legales.

c. Valoración crítica y límites del instrumento

Finalmente, el Reglamento introduce una modificación significativa en la aplicación de las medidas de diligencia debida, especialmente en relación con operadores jurídicos como notarios, abogados o agentes inmobiliarios contenida en el artículo 16. En los supuestos en los que dichos profesionales sean los únicos intervinientes en una operación, deberán aplicar las medidas exigidas respecto de ambas partes, y no solo respecto de su cliente directo. Esta previsión elimina una zona de sombra frecuente en los flujos de adquisición de activos o titularidades jurídicas, donde se canalizaban fondos opacos a través de relaciones trianguladas.

En suma, el Reglamento AML no sustituye al Derecho penal, ni tipifica conductas punibles, pero constituye una infraestructura normativa indispensable para su operatividad, al facilitar la detección temprana de patrones delictivos, habilitar el acceso a información clave y obligar a los actores del ecosistema cripto a colaborar con el sistema de control. Su eficacia, no obstante, dependerá de su coordinación efectiva con las disposiciones penales sustantivas, en particular las derivadas de la Sexta Directiva (UE)

¹³⁵ Vid. art. 3.1(1) del Reglamento MiCA, que define de forma detallada los servicios comprendidos bajo el concepto de proveedor de servicios sobre criptoactivos (CASP)

¹³⁶ Autoridad Bancaria Europea. (2022). *Directrices sobre políticas y procedimientos de cumplimiento normativo interno, funciones del AML/CFT compliance officer y papel del órgano de dirección o administración* (EBA/GL/2022/05. SEPBLAC. https://www.sepblac.es/wp-content/uploads/2022/09/Directrices_sobre_responsable_de_cumplimiento_ES.pdf)

2018/1673¹³⁷, y de su adaptación constante a fenómenos tecnológicos en rápida evolución como los servicios descentralizados (DeFi) o los activos autogestionados.

3.4.4. Normativa española: la Ley 10/2010

La Ley 10/2010, de 28 de abril, constituye el eje de la regulación nacional en materia de prevención del blanqueo de capitales, actuando como cauce de transposición de las sucesivas directivas europeas. En ella se reproducen, con adaptaciones, los principales mecanismos preventivos desarrollados en el marco comunitario, articulados bajo la supervisión del SEPBLAC como autoridad nacional competente.

A modo de cierre, puede afirmarse que la regulación administrativa europea en materia de prevención del blanqueo de capitales ha evolucionado hacia un sistema formalmente robusto y cada vez más inclusivo, capaz de incorporar a los actores del ecosistema cripto dentro del perímetro normativo. No obstante, su efectividad real frente a las nuevas formas de criminalidad digital dependerá de su capacidad para coordinarse con el sistema penal y de su adaptabilidad técnica ante entornos descentralizados, anónimos y en constante mutación. La prevención del blanqueo mediante criptoactivos exige no solo normas amplias, sino una infraestructura supervisora eficaz y una interpretación funcional que traduzca las obligaciones preventivas en mecanismos operativos concretos.

4. CARACTERÍSTICAS ESTRUCTURALES DE LOS CRIPTOACTIVOS QUE FAVORECEN SU USO COMO INSTRUMENTO DE BLANQUEO DE CAPITAL

El uso de criptoactivos en el contexto del delito de blanqueo de capitales no constituye simplemente una nueva forma de ejecutar viejas estrategias delictivas, sino que representa un desafío estructural que desborda el marco conceptual y normativo tradicional. Las propiedades que definen técnicamente a los criptoactivos, descentralización, pseudonimato, irreversibilidad, desintermediación, no son meros rasgos tecnológicos, sino factores jurídicamente disruptivos. Su combinación produce un entorno que tensiona los principios básicos del Derecho penal económico y de los sistemas de prevención financiera. Este apartado analiza críticamente dichas características desde una perspectiva penal, valorando en qué medida su configuración técnica obstaculiza o directamente inutiliza los mecanismos clásicos de detección, atribución e imputación penal del blanqueo.

4.1. Descentralización y desintermediación: la exclusión del control institucional

El tipo penal de blanqueo exige dolo: conocimiento del origen ilícito y voluntad de encubrir o integrar el dinero en el sistema. La utilización de criptoactivos plantea problemas en la reconstrucción de este elemento subjetivo, debido a la dificultad para identificar al sujeto interviniente. La mayoría de los criptoactivos permiten operar sin verificar la identidad del titular de una wallet, especialmente en entornos no custodiados

¹³⁷ Directiva (UE) 2018/1673, op. cit.

ni centralizados. Así, aunque la operación esté registrada en la blockchain, no es posible establecer quién la realizó, lo que impide imputar penalmente con certeza la conducta¹³⁸.

Este fenómeno no es exclusivo del entorno digital: también el efectivo carece de nominatividad. Sin embargo, el criptoactivo añade un grado de complejidad al hacer posible operar globalmente sin presencia física, sin documentación, sin fronteras y sin intermediarios. Como advierte la doctrina, este entorno no es anónimo, pero sí jurídicamente opaco en cuanto a la acreditación probatoria del conocimiento del origen delictivo¹³⁹.

4.2. La desintermediación y sus implicaciones para la prevención y detección

El sistema bancario tradicional constituye el eje del modelo preventivo establecido en la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo. Este modelo se basa en la existencia de sujetos obligados (art. 2), que actúan como puntos de control jurídico e institucional del sistema financiero. Estos operadores están legalmente obligados a identificar al cliente, aplicar medidas de diligencia debida, conservar documentos, analizar riesgos, y comunicar operaciones sospechosas al SEPBLAC¹⁴⁰.

Sin embargo, el ecosistema de criptoactivos, especialmente en su vertiente descentralizada, rompe esa arquitectura regulatoria. Buena parte de los operadores que intervienen en el tráfico cripto, como las wallets autocustodiadas, los protocolos DeFi, o las transacciones peer-to-peer, no se encuentran sometidos a obligaciones de compliance, ya que no tienen sede, forma jurídica definida o domicilio fiscal. La blockchain no requiere de bancos, ni de plataformas reguladas, ni de ninguna entidad que actúe como sujeto obligado, lo que significa que las operaciones se realizan fuera del perímetro institucional de supervisión¹⁴¹.

Incluso cuando intervienen exchanges centralizados, muchos de ellos no están registrados en España ni en la UE, y no cumplen los requisitos de inscripción en el Registro del Banco de España previsto en la Disposición adicional segunda de la Ley 10/2010 (modificada por la Ley 7/2021)¹⁴². A ello se suma la problemática de que el usuario puede saltar entre plataformas reguladas y no reguladas, o incluso entre redes blockchain distintas, sin generar un rastro documental coherente desde el punto de vista jurídico.

Este fenómeno no solo afecta a la prevención, sino también a la capacidad reactiva del sistema penal. Aunque una investigación posterior logre vincular una dirección de blockchain a actividades ilícitas, no existe, en la mayoría de los casos, un registro documental que permita reconstruir la cadena de titularidad o justificar el origen de los fondos¹⁴³. A diferencia de una cuenta bancaria, donde existe contrato, copia del DNI,

¹³⁸ Ley 10/2010, *op. cit.*

¹³⁹ Chamorro Rodríguez, *op. cit.*

¹⁴⁰ Doménech Ariza, *op. cit.*, p. 48.

¹⁴¹ CNMV, *op. cit.*

¹⁴² Chamorro Rodríguez, *op. cit.*, p. 4.

¹⁴³ Tapia Hermida, *op. cit.*, p. 20.

datos de movimientos y un sistema de alertas, en muchos entornos cripto no queda constancia identificativa alguna más allá de una dirección alfanumérica¹⁴⁴.

Desde una perspectiva funcional, esta quiebra del principio de trazabilidad institucional implica que el Estado no tiene ni la capacidad preventiva ni los medios probatorios que sí posee en el sistema financiero tradicional, lo que convierte al ecosistema cripto en un entorno de riesgo sistémico para el control del blanqueo⁶.

4.3. Posibilidades de segmentación, diseminación y reconversión del capital

Una de las funcionalidades más destacadas de los criptoactivos en relación con el delito de blanqueo es su capacidad para facilitar la estratificación digital del capital, replicando y perfeccionando las técnicas clásicas del delito. La fase de diseminación o “layering” en el blanqueo tradicional implicaba mover los fondos ilícitos a través de múltiples operaciones financieras, jurídicas o territoriales, con el fin de ocultar su origen. En el entorno blockchain, esta fase puede ejecutarse de forma casi automática y a gran escala.

Los criptoactivos permiten la fragmentación del valor en múltiples operaciones pequeñas (microtransacciones), la conversión entre diferentes tokens o criptomonedas, por ejemplo, de Bitcoin a Monero, o a stablecoins como USDT, y el uso de plataformas descentralizadas que eliminan la necesidad de intermediarios identificables. Estas operaciones, además, pueden realizarse mediante contratos inteligentes programados para ejecutarse de forma anónima, sin intervención humana directa¹⁴⁵.

Un fenómeno particularmente relevante es el uso de mezcladores (mixers) y puentes entre blockchains (cross-chain bridges), que permiten transitar los fondos a través de diferentes redes con lógicas técnicas distintas, dificultando la reconstrucción jurídica de la trazabilidad. Según advierte la doctrina penal reciente, estas herramientas tienen la capacidad de romper la lógica probatoria, ya que incluso cuando se rastrea el capital desde su punto de origen, resulta prácticamente imposible demostrar su llegada a un destino ilícito concreto¹⁴⁶.

Esto genera un efecto jurídico adverso: aunque exista prueba del delito precedente y de la tenencia posterior del criptoactivo, no siempre es viable demostrar la conexión causal entre ambos. La jurisprudencia exige que el activo poseído provenga del delito precedente, no simplemente que el sujeto haya intervenido en ambas fases. Esta ruptura de la conexión lógica penal debilita gravemente la eficacia del tipo del art. 301 CP en contextos digitales¹⁴⁷.

Además, la capacidad de segmentación se ve potenciada por la posibilidad de emplear identidades digitales múltiples (múltiples wallets, proxies, redes privadas virtuales) que impiden incluso afirmar que un mismo sujeto ha ejecutado la cadena de movimientos. La combinación de estas herramientas permite una reconversión digital del capital que

¹⁴⁴ GAFI, *op. cit.*, p. 13.

¹⁴⁵ León Delgado, J., *op. cit.*, p. 17.

¹⁴⁶ Doménech Ariza, *op. cit.*, p. 51.

¹⁴⁷ Chamorro Rodríguez, *op. cit.*, p. 5.

supera en sofisticación y eficacia las estructuras fiduciarias o societarias empleadas tradicionalmente¹⁴⁸.

4.4. Comparación con el dinero en efectivo: ¿mayor o menor peligrosidad?

La doctrina penal y administrativa ha debatido si los criptoactivos suponen un riesgo adicional respecto al efectivo en el contexto del blanqueo. En principio, ambos sistemas comparten una característica clave: la ausencia de nominatividad. Ni el billete físico ni el token digital reflejan, en sí mismos, quién es su titular. Sin embargo, esta analogía es superficial, ya que los criptoactivos presentan funcionalidades técnicas que amplifican ese riesgo estructural¹⁴⁹.

En primer lugar, la capacidad de transacción sin límites espaciales ni temporales es sustancialmente superior. Mientras que transportar dinero físico en grandes cantidades implica riesgos logísticos, legales y de detección, los criptoactivos pueden enviarse en segundos y sin exposición física, incluso mediante algoritmos automatizados. No hay fronteras ni necesidad de declarar su paso por aduanas¹⁵⁰.

En segundo lugar, los criptoactivos permiten un control más preciso del anonimato, mediante el uso de herramientas tecnológicas como redes TOR, servicios DeFi, wallets sin custodia y mecanismos de ofuscación. Aunque el dinero físico también puede circular sin control, su uso masivo suele generar sospechas inmediatas (por ejemplo, pagos en efectivo por bienes inmuebles). En cambio, en el entorno cripto no existen alertas institucionalizadas si el movimiento se produce fuera del perímetro de los sujetos obligados¹⁵¹.

No obstante, también es cierto que los criptoactivos dejan, a diferencia del efectivo, un rastro técnico en la blockchain. La dificultad no está en la inexistencia de datos, sino en su desconexión con el plano jurídico-identificativo. Así, el reto no es la falta de trazabilidad material, sino la falta de trazabilidad jurídica. Por tanto, aunque desde un punto de vista técnico podrían facilitar la detección, desde el punto de vista jurídico-procesal resultan menos eficaces como prueba si no se logra vincular wallet y sujeto¹⁵².

En resumen, no se trata de decidir si los criptoactivos son “peores” que el efectivo, sino de reconocer que introducen nuevas lógicas y riesgos funcionales que el Derecho penal y administrativo aún no ha resuelto del todo. Su naturaleza digital, modular y transfronteriza exige una adaptación profunda de los mecanismos preventivos y represivos, sin que ello implique criminalizar la tecnología en sí misma.

4.5. Riesgos añadidos por el carácter irreversible y la dificultad de reacción estatal

Otro elemento relevante es la irreversibilidad de las operaciones en la mayoría de las blockchains. Una vez que una transacción ha sido validada y confirmada, no puede ser modificada ni revertida. Esto impide que, ante la sospecha de una operación de blanqueo,

¹⁴⁸ GAFI, *op. cit.*, p. 13.

¹⁴⁹ Tapia Hermida, *op. cit.*, p. 22.

¹⁵⁰ Parlamento Europeo, *op. cit.*, p. 34.

¹⁵¹ CNMV, *op. cit.*

¹⁵² Domínguez García, *op. cit.*, p. 11.

el sistema judicial pueda intervenir con medidas cautelares clásicas (embargo, bloqueo, cancelación)¹⁵³.

Además, muchos activos son transferidos inmediatamente a wallets no localizables o a jurisdicciones que no cooperan con investigaciones internacionales. Esto hace que la reacción estatal pierda eficacia frente al delito consumado, debilitando no solo la prevención, sino también la restauración del orden jurídico¹⁵⁴.

4.6. Conclusión: una herramienta de riesgo estructural

Los criptoactivos, por su diseño técnico, pueden facilitar conductas típicas del delito de blanqueo en cualquiera de sus fases, especialmente si se emplean fuera de marcos institucionalizados. La falta de identificación, la eliminación de intermediarios, la posibilidad de dispersar y reconvertir fondos rápidamente, y la imposibilidad de revertir operaciones consolidan su condición de instrumento de alto riesgo si no existe una regulación eficaz.

No cabe concluir que estas tecnologías sean intrínsecamente ilícitas. Sin embargo, sus características funcionales multiplican las dificultades prácticas para la atribución penal, la trazabilidad jurídica y la reacción del sistema. Ello justifica la necesidad de un tratamiento jurídico específico, tanto desde el Derecho penal como desde el marco regulador preventivo.

5. PROPUESTA DE LEGE FERENDA: ¿ES NECESARIO MODIFICAR O REFORZAR EL ACTUAL ART. 301 CP PARA SANCIONAR NUEVAS CONDUCTAS DE BLANQUEO?

5.1. Adecuación y límites del artículo 301 frente al Uso de Criptoactivos

El artículo 301 del Código Penal español presenta una formulación abierta y suficientemente flexible como para abarcar las nuevas modalidades de blanqueo derivadas del uso de criptoactivos. La conducta típica “adquirir, poseer, utilizar, convertir o transmitir bienes”, así como realizar “cualquier otro acto” que tenga como finalidad ocultar o encubrir su origen ilícito, se construye con términos amplios que no restringen el tipo a formas clásicas o a determinados tipos de bienes.

En este contexto, los criptoactivos pueden y deben entenderse incluidos en la noción de “bienes”, dado que representan valor económico, son transmisibles, intercambiables y utilizados como medio de pago o inversión. Así lo está reconociendo de forma creciente la doctrina y la jurisprudencia comparada. Además, la cláusula final del tipo —“cualquier otro acto para ocultar o encubrir su origen ilícito”— actúa como cláusula de cierre del injusto, y otorga al tipo una capacidad de adaptación normativa frente a técnicas nuevas o tecnológicamente avanzadas de blanqueo, como el uso de mixers, DeFi o tokens de privacidad.

¹⁵³ Domínguez García, *op. cit.*, p. 11.

¹⁵⁴ GAFI, *op. cit.*, p. 21.

Esto significa que el artículo 301 CP no necesita ser reformado para responder al fenómeno de los criptoactivos, porque ya contiene los elementos necesarios para sancionar su uso en operaciones de blanqueo. Las dificultades no son dogmáticas, sino instrumentales y probatorias: identificar a los autores, vincular el activo al delito precedente, y acreditar el elemento subjetivo.

Por tanto, no existen verdaderos “huecos” del tipo penal, sino limitaciones prácticas en su aplicación que deben resolverse mediante mecanismos de cooperación, desarrollo jurisprudencial y refuerzo del sistema administrativo, pero no mediante una reforma penal inmediata. En efecto, la literalidad del artículo 301 CP, y especialmente su cláusula final “cualquier otro acto para ocultar o encubrir su origen ilícito” permite una lectura amplia y evolutiva, capaz de absorber las nuevas formas de criminalidad económica asociadas a los criptoactivos.

Las principales dificultades no derivan del contenido del tipo, sino de condicionantes técnicos y estructurales: la opacidad de los entornos descentralizados, la ausencia de registros de identidad, la volatilidad de los activos, o la falta de colaboración entre jurisdicciones. Estos obstáculos hacen que, en la práctica, el tipo se aplique con menor eficacia, pero ello no revela una insuficiencia normativa, sino una falta de integración entre el plano penal, el sistema preventivo y la cooperación internacional.

Por eso, la respuesta más eficaz no pasa por reformular el artículo 301 CP, sino por fortalecer los sistemas complementarios que le dan operatividad: una jurisprudencia penal adaptada a la realidad tecnológica, una regulación administrativa robusta, como la que adelanta MiCA y una infraestructura internacional que facilite la trazabilidad jurídica. El Derecho penal no necesita extender su alcance, sino potenciar su capacidad de acción dentro del marco legal ya existente.

5.2. Capacidad del tipo penal para abordar las técnicas modernas de blanqueo.

El delito de blanqueo ha evolucionado de forma paralela a los medios utilizados por la delincuencia para ocultar el origen ilícito de los capitales. En este proceso, la incorporación de criptoactivos como herramienta ha transformado no solo los canales operativos, sino también las técnicas empleadas para disociar el bien del delito que lo origina. Ante esta realidad, resulta necesario valorar si el tipo penal del artículo 301 CP, aun siendo formalmente adecuado, es funcionalmente eficaz para perseguir las nuevas formas de actuación basadas en tecnología blockchain.

Muchas de las técnicas modernas de blanqueo que involucran criptoactivos —como el uso de mixers, exchanges descentralizados (DEX), contratos inteligentes para automatizar transacciones, y operaciones estructuradas entre múltiples tokens— no introducen conductas cualitativamente nuevas respecto al tipo penal, sino que replican viejas lógicas de ocultación mediante medios novedosos. La conversión, fragmentación, interposición de terceros o territorialización compleja ya existían en el blanqueo clásico, aunque ahora adquieren una dimensión de automatización, anonimato y descentralización sin precedentes.

La dificultad no radica en el encaje legal del tipo, ya abordado, sino en su aplicación frente a estructuras operativas descentralizadas y técnicamente complejas. La descentralización impide identificar fácilmente a los sujetos activos; la automatización,

mediante smart contracts, dificulta atribuir voluntad delictiva; y la multiplicidad de jurisdicciones plantea retos para la aplicación del principio de territorialidad y para la cooperación judicial. Ello compromete la eficacia práctica del tipo penal, que enfrenta limitaciones técnicas y probatorias propias de un entorno digital descentralizado.

En este escenario, el tipo penal necesita ser interpretado no solo de forma extensiva (dentro de los márgenes de la legalidad), sino también desde una lógica funcional y finalista: lo relevante no es tanto el instrumento técnico utilizado, sino si el comportamiento perseguía una finalidad típica de ocultación o encubrimiento. Por ejemplo, el uso de una aplicación de intercambio descentralizado no debería quedar fuera del tipo si esa operación tenía como fin disociar el activo de su origen ilícito.

La capacidad del artículo 301 CP para abordar estas nuevas técnicas depende, en última instancia, de una interpretación jurisprudencial que tenga en cuenta los elementos sustanciales del injusto: intención de ocultación, conocimiento del origen delictivo y voluntad de integración en el circuito lícito. Solo de este modo puede mantenerse la vigencia del tipo frente a prácticas que cambian rápidamente en su forma, pero no en su sustancia.

5.3. La insuficiencia parcial del marco administrativo-preventivo

La eficacia de la lucha contra el blanqueo de capitales no se agota en la represión penal, sino que depende esencialmente de la eficacia del sistema preventivo-administrativo. En el ámbito europeo, este sistema se articula fundamentalmente en torno a dos pilares: el Reglamento MiCA y la normativa contra el blanqueo de capitales (AML). No obstante, ambos instrumentos, a pesar de su voluntad reguladora, presentan serias limitaciones estructurales y funcionales cuando se trata de aplicar sus mecanismos a los criptoactivos.

El Reglamento MiCA supone el primer intento europeo serio de dotar de un marco jurídico integral al mercado de criptoactivos. Introduce la figura de los proveedores de servicios de criptoactivos (CASP), impone exigencias de autorización, y prevé mecanismos de control y supervisión por parte de las autoridades nacionales y de la ESMA.

Sin embargo, MiCA no cubre todo el ecosistema cripto. Deja fuera:

- Los activos puramente descentralizados, que operan sin entidad emisora ni intermediarios centralizados.
- Los NFTs (salvo que cumplan funciones de inversión o pago repetido).
- Los protocolos de DeFi, donde no hay proveedor de servicios definido, sino código abierto desplegado en la blockchain.

Esta realidad genera una zona de sombra regulatoria, especialmente peligrosa, ya que precisamente estos entornos son los que presentan mayor opacidad y riesgo de utilización para el blanqueo. Además, la plena aplicabilidad de MiCA está aún en desarrollo, lo que acentúa la sensación de incertidumbre normativa.

Por otro lado, las sucesivas Directivas AML han intentado adaptarse al mundo cripto exigiendo la identificación del cliente, el registro de operaciones y la comunicación de actividades sospechosas. Sin embargo, estas obligaciones se aplican únicamente a los

sujetos obligados formalmente registrados, como los CASP regulados o los exchanges centralizados.

En cambio, no existe una cobertura real para las actividades realizadas mediante wallets autocustodiadas, plataformas peer-to-peer, mixers o contratos inteligentes sin emisor identificable. En estos casos, las medidas AML simplemente no se aplican, no por falta de voluntad normativa, sino por ausencia de un sujeto jurídicamente responsable que pueda ser vigilado.

Además, la aplicación práctica de estas medidas varía drásticamente entre Estados miembros, lo que impide una supervisión uniforme y facilita el arbitraje regulatorio. Esta fragmentación también complica la cooperación transfronteriza, esencial en un mercado global como el de los criptoactivos.

En síntesis, tanto MiCA como el marco AML europeo representan avances importantes, pero no logran abarcar con eficacia el núcleo más problemático del ecosistema cripto, que opera precisamente fuera del radar de los sujetos obligados tradicionales. Esta limitación no es solo normativa, sino estructural: las medidas de prevención actuales no son funcionalmente aplicables a los entornos puramente descentralizados, lo que abre grietas significativas en el sistema preventivo.

Por ello, no puede pretenderse que el Derecho penal supla estas carencias mediante una expansión del tipo, sino que es necesario reforzar el marco administrativo, ampliar la supervisión técnica y promover una arquitectura europea coordinada que no deje espacios de impunidad en el mundo cripto.

5.4. ¿Reformar el tipo penal? Argumentos para una respuesta negativa

El análisis realizado a lo largo de este capítulo permite sostener con claridad que el artículo 301 del Código Penal español no requiere una reforma sustancial para hacer frente al fenómeno del blanqueo de capitales mediante criptoactivos. La redacción del tipo es suficientemente amplia, flexible y tecnológicamente neutra como para incluir dentro de su alcance las nuevas formas de conversión, ocultación o encubrimiento de bienes digitales, en tanto estas reproduzcan la finalidad típica del delito.

No obstante, el reto actual no es normativo, sino funcional: reside en la capacidad del sistema penal y, especialmente, del sistema preventivo-administrativo, para operar eficazmente en entornos altamente descentralizados, anónimos y técnicamente complejos. Como se ha argumentado, ni el Reglamento MiCA ni las Directivas AML logran aún cubrir aquellas zonas del ecosistema cripto donde no existen sujetos obligados, lo que debilita la trazabilidad de operaciones y la identificación de los intervinientes.

En este contexto, se proponen tres grandes líneas de actuación:

- Consolidar una interpretación jurisprudencial funcional del artículo 301 CP, orientada a valorar la intención de ocultación más allá del instrumento técnico empleado, sin necesidad de reformar el tipo penal ni crear nuevos subtipos específicos.

- Reforzar el marco administrativo-preventivo, ampliando las obligaciones de vigilancia y reporte a nuevos actores del entorno cripto (como desarrolladores de protocolos DeFi, operadores de mixers o plataformas de NFT que asuman funciones económico-financieras), sin limitarse a los proveedores de servicios centralizados.
- Avanzar hacia una arquitectura europea verdaderamente integrada, que armonice los estándares AML, mejore la supervisión técnica transfronteriza, y reduzca los márgenes de arbitraje normativo que hoy permiten desplazar actividades ilícitas a jurisdicciones más laxas.

Desde esta perspectiva, la implementación de los criptoactivos en el delito de blanqueo de capitales no ha generado un nuevo tipo de delito, sino que ha introducido una nueva herramienta tecnológica al servicio de un delito tradicional. La respuesta jurídica no debe pasar por una hiperactividad legislativa en el plano penal, sino por una lectura transversal, especializada y coordinada de los instrumentos ya disponibles.

Solo desde esta lógica sistémica es posible preservar la seguridad jurídica, garantizar la eficacia en la persecución del delito, y evitar la expansión innecesaria del Derecho penal más allá de sus límites legítimos.

6. RESUMEN DE CONCLUSIONES

El análisis desarrollado a lo largo de este trabajo ha permitido profundizar en las múltiples implicaciones que conlleva el uso de criptoactivos en el ámbito del delito de blanqueo de capitales. A partir del estudio conjunto del marco penal y del sistema preventivo-administrativo, se ha podido constatar que los verdaderos desafíos no derivan tanto de un vacío normativo, sino de la necesidad de reinterpretar y reconfigurar las herramientas jurídicas existentes para responder eficazmente a una realidad tecnológica en transformación constante.

Los criptoactivos no han dado lugar, en sí mismos, a una nueva figura delictiva. Su novedad reside en las particularidades técnicas que introducen en los procesos de blanqueo: descentralización, pseudoanonimato, desintermediación, automatización mediante contratos inteligentes, y circulación global instantánea. Estas propiedades no modifican la estructura típica del delito, pero sí dificultan su investigación, prueba e imputación. En ese sentido, se ha sostenido que el artículo 301 del Código Penal español, en su configuración actual, posee la flexibilidad y amplitud necesarias para abarcar estas nuevas modalidades operativas, siempre que sea interpretado de manera finalista y funcional. La clave reside en desplazar el foco desde el instrumento utilizado hacia la voluntad de ocultación y disociación que constituye el núcleo del injusto penal.

Sin embargo, el trabajo también ha puesto de manifiesto que la eficacia del Derecho penal frente al blanqueo con criptoactivos depende en gran medida del correcto funcionamiento del sistema preventivo, tanto a nivel nacional como supranacional. Si bien la Ley 10/2010 ha avanzado en la inclusión de operadores cripto como sujetos obligados, y el Reglamento MiCA ha comenzado a establecer un marco común europeo, la realidad es que una parte sustancial del ecosistema cripto queda aún fuera de supervisión efectiva. Plataformas descentralizadas, wallets no custodiadas y herramientas como mixers o protocolos DeFi

siguen operando sin controles, sin identificación de usuarios, y sin canales efectivos de reporte.

Las medidas de prevención recogidas en las normas AML resultan difíciles de aplicar allí donde no hay un sujeto jurídicamente responsable al que imponer obligaciones. Esta situación no solo genera espacios de impunidad, sino que debilita la capacidad de los sistemas judiciales para recopilar pruebas que permitan la activación del mecanismo penal. En consecuencia, la eficacia del artículo 301 CP se ve afectada indirectamente por la debilidad del sistema preventivo, lo que confirma que el problema no es tanto de norma penal, sino de estructura institucional.

En este escenario, se rechaza la necesidad de una reforma inmediata del tipo penal. Lejos de contribuir a la solución, una modificación del artículo 301 podría generar efectos indeseados de inseguridad jurídica o sobreactuación punitiva. La respuesta jurídica más adecuada pasa por reforzar el sistema existente a través de tres líneas prioritarias: En primer lugar, desarrollar criterios jurisprudenciales sólidos que permitan adaptar la interpretación del tipo a la realidad digital sin vulnerar garantías. En segundo lugar, ampliar la supervisión técnica y legal de los actores cripto, dotando de mecanismos de control a espacios que hoy escapan a la regulación efectiva. Y en tercer lugar, impulsar una verdadera armonización normativa europea, que evite arbitrajes regulatorios y asegure una cooperación judicial eficiente.

En definitiva, la lucha contra el blanqueo de capitales en el entorno cripto no exige una expansión del Derecho penal, sino una respuesta jurídica inteligente y especializada, basada en la integración de saberes técnicos, la mejora de la capacidad institucional y el respeto al principio de intervención mínima. Solo así podrá mantenerse un equilibrio entre eficacia represiva, seguridad jurídica y protección de las libertades fundamentales en el nuevo contexto digital.

7. BIBLIOGRAFÍA

1) LEGISLACIÓN

Código Civil español, arts. 333, 335, 337 y 1255.

Código Penal español, art. 301.

Consejo de Europa. (1990). Convenio relativo al blanqueo, detección, embargo y decomiso de los productos del delito, art. 1.

Consejo de la Unión Europea. (1991). Directiva 91/308/CEE, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales. DOCE L 166/77. [ELI: <https://eur-lex.europa.eu/legal-content/ES/ELI/DIR/1991/308/oj>]

Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014. DOUE L 173, 12 de junio de 2014, pp. 349–496.

Directiva (UE) 2018/1673, de 23 de octubre de 2018, sobre la lucha contra el blanqueo de capitales mediante el Derecho penal. DOUE L 284, 12 de noviembre de 2018, arts. 3.4 y 5. [ELI: <https://eur-lex.europa.eu/legal-content/ES/ELI/DIR/2018/1673/oj>]

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Boletín Oficial del Estado, 103, de 29 de abril de 2010. ELI: <https://www.boe.es/eli/es/l/2010/04/28/10>

Naciones Unidas. (1988). Convención contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas (Convención de Viena), art. 1.q.

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023. DOUE, art. 2.

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, arts.

2) JURISPRUDENCIA

Tribunal Supremo, Sala Primera. (1965). Sentencia de 6 de marzo (RJ 1965/1124).

Tribunal Supremo, Sala de lo Penal. (2000). Sentencia 1637/2000, de 10 de enero (RJ 2000/1637), FJ 5.º.

Tribunal Supremo, Sala de lo Penal. (2001). Sentencia 2410/2001, de 18 de diciembre (RJ 2001/10457), FJ 4.º.

Tribunal Supremo, Sala de lo Penal. (2005). Sentencia 924/2005, de 17 de junio, FJ 4.º.

Tribunal Supremo, Sala de lo Penal. (2006). Sentencia 928/2006, de 5 de octubre (RJ 2006/6937), FJ 11.º.

Tribunal Supremo, Sala de lo Penal. (2007). Sentencia 457/2007, de 29 de mayo, FJ 3.º.

Tribunal Supremo, Sala de lo Penal. (2011). Sentencia 156/2011, de 21 de marzo, FJ 3.º.

Tribunal Supremo, Sala Segunda. (2014). Sentencia 56/2014, de 6 de febrero, FJ 2.º.

Tribunal Supremo, Sala de lo Penal. (2015). Sentencia 265/2015, de 29 de abril, FJ 9.º.

Tribunal Supremo, Sala Segunda. (2019). Sentencia 326/2019, de 20 de junio, FJ 3.º.

Tribunal Supremo. (2019). Sentencia 501/2019, de 24 de octubre (RJ 2019/501).
 Tribunal Supremo. (2021). Sentencia 4523/2021 (RJ 2021/4523).
 Tribunal Supremo. (2022). Sentencia 2456/2022, de 16 de junio (RJ 2022/2456).

3) OBRAS DOCTRINALES

Álvarez González, J. (2019). *Blanqueo de capitales: cinco parámetros de reducción teleológica a la luz de la jurisprudencia del Tribunal Supremo*. Tesis doctoral. Universidad Complutense de Madrid.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (2.^a ed.). O'Reilly Media.

Barrio Andrés, M. (2022). “La nueva regulación de los criptoactivos en España”. *Diario La Ley*, (10010).

Blanco Cordero, I. (2015). *El delito del blanqueo de capitales* (4.^a ed.). Aranzadi.

Blanco Cordero, I., Fabián Caparrós, E., Prado Saldarriaga, V., Santander Abril, G., & Zaragoza Aguado, J. (2018). *Combate al lavado de activos desde el sistema judicial*. OEA, pp. 136–143. Cizur Menor: Aranzadi, p. 232.

Chamorro Rodríguez, M.^a de la C. (2019). *Aspectos jurídicos de las criptomonedas*. Blockchain Intelligence.

Cereijo Comet, M. (2018). *Análisis de la blockchain y de las criptomonedas: Relación con el delito de blanqueo de capitales*. TFG. Universidad Pontificia Comillas.

Del Carpio Delgado, J. (2016). “Sobre la necesaria interpretación y aplicación restrictiva del delito de blanqueo de capitales”. *InDret*, n.º 4.

Díaz-Maroto y Villarejo, J. (2017). “El lavado de activos o blanqueo de capitales y su regulación en España”. *Revista Peruana de Ciencias Penales*, (31), 133–170. <https://doi.org/10.31381/rpcp.v0i31.1435>

Dolader, J., Bel, J., & Muñoz, J. (2016). “La blockchain: fundamentos, aplicaciones y relación con la economía digital”. *Revista de Economía Industrial*, (405), 11–20.

González, A. (2021). “Blockchain como inicio de la revolución tecnológica del sector financiero”. En Corchado, J. M., & Tejedor, J. L. (Eds.), *C1b3rWall Academy - Módulo 0*. Universidad de Salamanca.

Hijas Cid, E. (2016). “Bitcoins: algunas cuestiones jurídicas”. *El Notario del Siglo XXI*, (66), 38–41.

Ibáñez Jiménez, J. W. (2018). *Blockchain: primeras cuestiones en el ordenamiento español*. Dykinson.

Lacruz Berdejo, J. L., Luna Serrano, A., & Rivero Hernández, F. (2005). *Elementos de Derecho civil*, tomo I, vol. 3. Thomson-Civitas.

Legerén-Molina, A. (2019). “Retos jurídicos que plantea la tecnología de la cadena de bloques”. *Revista de Derecho Civil*, 6(1), 177–237.

León Bazán, Y. Y., & Delgado Guerrero, J. S. (2024). “Contratos inteligentes a partir de una especificación semiformal”. *Revista Mikarimin*, 10(3), 31–42.

Martínez Boada, J., & Rejas Muslera, R. (2024). “Protección jurídica de Blockchain”. *Revista Chilena de Derecho y Tecnología*, 13, e73869.

Mir Puig, S. (2020). *Derecho penal. Parte general* (11.^a ed.). Barcelona: Reppertor

Jurídico, p. 152.

Muñoz Conde, F. (2012). *Derecho Penal. Parte especial* (3.^a ed.). Tirant lo Blanch.

Nieto Martín, A. (2019). *Responsabilidad penal de la persona jurídica*. Tirant lo Blanch.

Navarro Cardoso, F. (2019). “Criptomonedas y blanqueo de dinero”. *RECP*, (21), 13–16.

Orts Berenguer, E., & González Cussac, J. (2020). *Introducción al Derecho Penal. Parte general*. Tirant lo Blanch.

Palma Herrera, J. M. (2000). *Los delitos de blanqueo de capitals*. Edersa.

Peña Bernaldo de Quirós, M. (1999). *Derechos Reales. Derecho Hipotecario*. CRPME.

Pérez Marín, M. Á. (2023). “El reglamento MiCA: responsabilidad y sanción frente al incumplimiento de la regulación”. *Ius et Scientia*, 9(2), pp. 64–92. <https://doi.org/10.12795/IESTSCIENTIA.2023.i02.04>

Pieters, G., & Vivanco, S. (2015). *Bitcoin arbitrage and unofficial exchange rates*.

Preukschat, A. (2017). *Blockchain: la revolución industrial de internet*. Gestión 2000.

Puente González, I. A. (2020). “Criptomonedas y Derecho civil patrimonial”. *Diario La Ley*, (9619), p. 29.

Ramos Gil de la Haza, A. (2022). “La web3: una aproximación jurídica”. *Revista Jurídica Pérez-Llorca*, (8), p. 24.

Rodríguez Quejido, V. (2019). *Criptoactivos: naturaleza, regulación y perspectivas*. Instituto de Estudios Fiscales.

Saldaña Taboada, P. (2023). *Análisis criminológico de la delincuencia con criptomonedas*. Tesis doctoral. Universidad de Granada.

Samar Violeta, F. A., & Olmedo Cardente, M. D. (2024). “Enfoques regulatorios internacionales”. *Cuadernos de Política Criminal*, (143), p. 184.

Schuller, R. R. (2022). “Criptoactivos: Categorización jurídica”. *Cuadernos de Derecho Transnacional*, 14(2), 1129–1145.

Suárez Puga, E. A. (2020). *Naturaleza y régimen jurídico de las criptomonedas*. UPF y ESADE Law School.

Uría Menéndez. (2018). “Monedas virtuales: Aproximación jurídico-tributaria y control tributario”. *Actualidad Jurídica Uría Menéndez*, (48), 72–81.

4) RECURSOS DE INTERNET

Agencia Española de Protección de Datos & Supervisor Europeo de Protección de Datos. (2019). *Introducción al hash...* <https://www.edps.europa.eu/>

Autoridad Bancaria Europea. (2022). *Directrices sobre políticas y procedimientos de cumplimiento normativo interno, funciones del AML/CFT compliance officer y papel del órgano de dirección o administración* (EBA/GL/2022/05). SEPBLAC. https://www.sepblac.es/wp-content/uploads/2022/09/Directrices_sobre_responsable_de_cumplimiento_ES.pdf

BBVA. (2021). ¿Qué son los mercados over the counter

(OTC)? <https://www.bbva.com/es/que-son-los-mercados-over-the-counter-otc/> [consulta: 8 de mayo de 2025]

Consejo de la Unión Europea. (2024, 30 de mayo). *Lucha contra el blanqueo de capitales: el Consejo adopta un paquete de normas* [Nota de prensa]. <https://www.consilium.europa.eu/es/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/>

Comisión Europea. (2021, 20 de julio). *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules* [Nota de prensa]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

Comisión Nacional del Mercado de Valores (s.f.). *Regulación de los criptoactivos: Reglamento MiCA*. CNMV. <https://www.cnmv.es/Portal/mica/regulacion-criptoactivos?lang=es>

Dai, W. (1998). *b-money*. <http://www.weidai.com/bmoney.txt>

EBA & ESMA. (2025). *Joint Report on recent developments in crypto-assets*. Brussels: EU Publications.

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: EU Law Enforcement Agency.

FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

GAFI-FATF. (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. París: Financial Action Task Force.

Grupo de Acción Financiera Internacional (GAFI). (2012). *Las 40 recomendaciones del GAFI*. <https://www.fatf-gafi.org/>

Grupo de Acción Financiera Internacional (GAFI). *Glosario de términos clave*. <https://www.fatf-gafi.org>

GAFI. (2023). *Revisión de la función de las FIUs*. <https://www.fatf-gafi.org/>

Internal Revenue Service (IRS). (2014). *Notice 2014-21: Guidance on Virtual Currency*. <https://www.irs.gov/>

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>

Rodríguez Quejido, V. (2019). *Criptoactivos: naturaleza, regulación y perspectivas*. <https://www.ief.es/>

Saldaña Taboada, P. (2023). *Tesis doctoral*. <https://hdl.handle.net/10481/81413>

Suárez Puga, E. A. (2020). *Naturaleza y régimen jurídico de las criptomonedas*. <https://www.pensamientopenal.com.ar/>