Estudios de Deusto

Revista de Derecho Público

CONSIDERACIONES SISTEMÁTICAS SOBRE EL BLANQUEO DE CAPITALES Y FIGURAS DELICTIVAS AFINES EN EL ÁMBITO DE LOS CRIPTOACTIVOS

Systematic Considerations on Money Laundering and Related Criminal Offences in the Field of Cryptoassets

Samar Violeta Francisco Agra

https://doi.org/10.18543/ed.3751

Fecha de recepción: 02.03.2026 • Fecha de aceptación: 03.08.2026
Fecha de publicación anticipada en línea: noviembre 2026

Derechos de autores/as y Acceso Abierto

Se recomienda a las personas autoras que lean atentamente sus derechos. Creemos que este enfoque garantiza un acuerdo justo para ambas partes. Estas instrucciones se leen conjuntamente con el Código Ético y la Política de Acceso Abierto, Licencia y Derechos de Autor/a de la revista "Estudios de Deusto. Revista de Derecho Público".

1. Autoría y ética

Al entregar sus manuscritos a **Estudios de Deusto. Revista de Derecho Público,** los/las autores/as aceptan y se comprometen a cumplir las condiciones de publicación sin necesidad de firmar un documento de cesión adicional con la **Editorial (Universidad de Deusto).** Con ello, garantizan que su trabajo es inédito en cualquier forma, original y que no vulnera el Código Ético de la Revista ni

Copyright and Open Access

The authors are advised to read their rights carefully. We believe this approach ensures a fair agreement for both parties. These instructions should be read in conjunction with the Ethical Guidelines and the Open Access Policy, Licensing Terms and Copyright of the journal "Estudios de Deusto. Revista de Derecho Público".

1. Authorship and Ethics

By submitting their manuscripts to **Estudios de Deusto. Revista de Derecho Público**, the authors accept and undertake to comply with the conditions of publication without the need to sign an additional transfer agreement with the **Publisher (University of Deusto)**. In doing so, they guarantee that their work is unpublished in any form, original, and does not breach the Journal's Ethical Guidelines

derechos de terceros, y que no se han otorgado ni se otorgarán licencias que resulten incompatibles con los derechos concedidos a la Editorial.

Los/las autores/as asumen la responsabilidad total y exclusiva sobre el contenido de su estudio y declaran formalmente no tener conflictos de interés que afecten la integridad de la investigación.

2. Derechos de la Editorial

Al enviar el manuscrito, los/las autores/as aceptan su publicación bajo la licencia **Creative Commons CC BY-NC-ND 4.0**. En consecuencia, conceden a la Editorial el **derecho exclusivo, gratuito y universal para la primera publicación**, edición, maquetación y explotación de la obra. Esta concesión autoriza a la Editorial a distribuir, sublicenciar e indexar el trabajo en cualquier formato, medio, base de datos o repositorio institucional, con fines de promoción y difusión científica.

3. Derechos de autores/as

Los/las autores/as **conservan la propiedad intelectual de su obra y retienen el derecho a distribuir y utilizar su trabajo** para fines docentes, investigación futura o archivo personal, siempre que se cite la publicación original en la Revista. Se les permite además la publicación posterior en otros medios, siempre que se incluya una nota a pie de página con la referencia completa de la Revista (incluyendo el DOI, si está disponible) y no se sugiera el respaldo explícito de la Revista y/o Editorial.

4. Acceso abierto

Estudios de Deusto. Revista de Derecho Público es una revista de acceso abierto; lo que significa que es de libre y total acceso en su integridad inmediatamente después de la publicación de su contenido. No obstante, de acuerdo con la licencia arriba mencionada, se debe citar siempre a los/las autores/as de los artículos. Tanto su uso comercial como cualquier modificación que se pretenda distribuir requerirán el permiso expreso previo por escrito de quien sea titular de los derechos.

or the rights of third parties, and that no licences have been or will be granted that are incompatible with the rights granted to the Publisher.

The authors assume full and exclusive responsibility for the content of the study and formally declare that they have no conflicts of interest that affect the integrity of the research.

2. Publisher's Rights

By submitting the manuscript, the authors agree to its publication under the **Creative Commons CC BY-NC-ND 4.0** licence. Consequently, they grant the Publisher the **exclusive, royalty-free and worldwide right of first publication**, editing, layout and exploitation of the article. This grant authorises the Publisher to distribute, sub-license and index the work in any format, medium, database or institutional repository, for the purposes of promotion and scientific dissemination.

3. Copyright

The authors **retain the intellectual property rights to their article and retain the right to distribute and use their work** for teaching purposes, future research or personal archiving, provided that the original publication in the Journal is cited. They are also permitted to republish in other media, provided that a (foot)note is included with the full reference to the Journal (including the DOI, where available) and no explicit endorsement of the Journal and/or Publisher is implied.

4. Open Access

Estudios de Deusto. Revista de Derecho Público is an open-access journal; this means that it is freely and fully accessible in its entirety immediately upon publication of its content. However, in accordance with the licence mentioned above, the authors of the articles must always be properly cited; and both commercial use and any modification intended for distribution will require the express prior written permission of the rights holder.

CONSIDERACIONES SISTEMÁTICAS SOBRE EL BLANQUEO DE CAPITALES Y FIGURAS DELICTIVAS AFINES EN EL ÁMBITO DE LOS CRIPTOACTIVOS[1]

Systematic Considerations on Money Laundering and Related Criminal Offences in the Field of Cryptoassets

Samar Violeta Francisco Agra[2]
Período de Orientación Postdoctoral (FPU)
Universidad de Granada, Granada. España
https://orcid.org/0009-0004-3619-7201

https://doi.org/10.18543/ed.3751

Fecha de recepción: 02.03.2026
Fecha de aceptación: 03.08.2026
Fecha de publicación anticipada en línea: noviembre 2026

Resumen

Este artículo aborda los desafíos que plantea el uso de criptomonedas en la ejecución del blanqueo de capitales. Se analiza cómo estos activos virtuales facilitan cada

[1] Esta investigación se enmarca en la ejecución de los siguientes proyectos: "La relevancia de las remesas en el marco del fenómeno migratorio y de los comportamientos delictivos cometidos con criptomonedas" (PPJIB2023-010), ya finalizado, del cual la autora de este trabajo ha sido investigadora principal (IP), financiado por el Plan Propio de Investigación de la Universidad de Granada, y "Análisis cualitativo y fenomenológico de las amenazas cibernéticas a infraestructuras críticas nucleares y su impacto en la protección radiológica" (PRY015/23), en el que aquella forma parte del equipo de investigación, financiado por el Consejo de Seguridad Nuclear. Se agradece expresamente al Prof. Dr. Miguel Domingo Olmedo Cardenete, Catedrático de Derecho Penal de la Universidad de Granada e IP del segundo proyecto, por sus sugerencias y la revisión inicial de este trabajo.

[2] Email: samarfr@ugr.es

etapa del proceso de blanqueo y la perpetración de tradicionales delitos previos, como la receptación, la corrupción y el fraude fiscal. Se examina la tipificación del delito de blanqueo en España y se destacan los riesgos emergentes asociados a las finanzas descentralizadas, las ofertas iniciales de proyectos cripto, los tokens no fungibles, los servicios mezcladores, entre otros. No solo se proponen soluciones jurídicas, sino que se destacan propuestas técnico-informáticas para la persecución del delito, porque la opacidad y descentralización de las criptomonedas dificultan significativamente la capacidad de las autoridades para investigar y sancionar eficazmente estas conductas ilícitas.

Palabras clave

Blanqueo de capitales, receptación, corrupción, fraude fiscal, criptodelitos, criptomonedas, criptoactivos.

Abstract

This article addresses the challenges posed by the use of cryptocurrencies in money laundering. It analyses how these virtual assets facilitate each stage of the laundering process and the commission of traditional predicate offenses such as receiving stolen goods, corruption, and tax fraud. The criminalization of money laundering in Spain is examined, highlighting emerging risks associated with decentralized finance, initial coin offerings, non-fungible tokens, mixing services, among others. Not only legal solutions are proposed, but also technical and informatic approaches for crime enforcement are emphasized, since the opacity and decentralization of cryptocurrencies significantly hinder authorities' ability to effectively investigate and prosecute these illicit activities.

Keywords

Money laundering, handling stolen goods, corruption, tax fraud, cryptocrimes, cryptocurrencies, cryptoassets.

Sumario: I. Aproximación jurídico-penal al blanqueo de capitales y las criptomonedas. II. Fases del blanqueo de capitales y su reconocimiento cuando median criptomonedas. 1. Fase de colocación. 2. Fase de estratificación. 3. Fase de integración. III. Delitos relacionados con el blanqueo de capitales y criptomonedas. 1. La receptación. 2. El delito fiscal. 3. La corrupción pública. 4. La corrupción privada. IV. Problemáticas específicas asociadas a la persecución del blanqueo de capitales cuando intervienen criptoactivos. 1. Los "muleros". 2. Las *Initial Coin Offerings* (ICOs). 3. Las *self-custody wallets*. 4. El método *proof-of-burn*. 5. Los *Non-Fungible Tokens* (NFT). V. Conclusiones. VI. Referencias bibliográficas.

I. APROXIMACIÓN JURÍDICO-PENAL AL BLANQUEO DE CAPITALES Y LAS CRIPTOMONEDAS

El blanqueo de capitales —también conocido como lavado de activos, aunque es frecuente la utilización de esta forma terminológica en Latinoamérica— consiste en un proceso con el que se intenta que el dinero obtenido de actividades ilegales parezca legítimo o provisto por fuentes legales. De esta forma, se introducen en el tráfico económico legal beneficios generados por la perpetración de delitos (Vidales Rodríguez, 2015: ep. 1[3]), razón por la cual los efectos dañosos del blanqueo minan la credibilidad del sistema financiero (Souto, 2024: p. 726). Mezclar bienes sometidos a las reglas del ordenamiento jurídico con otros que afloran sin cumplir dichas reglas es un problema para el orden socioeconómico (Martín Sagrado, 2018: p. 13). Por eso, aunque un sector de la doctrina ha intentado proponer otras alternativas[4], gran parte de ella coincide en que el bien jurídico protegido por el delito de blanqueo de capitales es precisamente ese, el orden socioeconómico. Aunque la noción de "bien jurídico" es vaga e indeterminada, el TS[5] aclara que dentro de ella se inserta 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, y que

[3] De ahí que la autora destaque que se trata de una manifestación criminal que acapara gran atención a nivel mundial.

[4] Por ejemplo, Bacigalupo Saggese & Bajo Fernández (2010: p. 678); proponen que el bien jurídico protegido por el delito de blanqueo es coincidente con el del delito precedente, pues aquella conducta solo agrava o mantiene la lesión de la segunda.

[5] STS 279/2013, 6 de Marzo de 2013, FJ 9. Además, que el blanqueo se tipifique dentro del Título relativo a los delitos contra el orden socioeconómico es otro indicio de que hacia la protección del mismo se orienta.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

afectan también al buen funcionamiento del mercado y de los mecanismos financieros y bursátiles"[6].

Al tratarse de un delito de referencia (Olmedo Cardenete, 2024: p. 929), el blanqueo se produce necesariamente tras la comisión de otro/s delito/s, de donde se obtuvieron los beneficios ilícitos. Dicho comportamiento criminal previo puede ser el tráfico de drogas, el robo con violencia, la extorsión, la trata de personas, las estafas, entre otros. Todos ellos son delitos donde existe ya un lucro y su aprovechamiento criminal. Para condenar por blanqueo de capitales, es necesario que se facilite "la introducción en el mercado regular de unos fondos que necesitan ser lavados por tener su origen en un delito antecedente" (STS 224/2024, FJ 2). Esto es importante porque, de lo contrario, se acabaría condenando a cualquier criminal dos veces solo por el hecho de mantener en su posesión o no entregar los fondos que obtuviese con actividades ilegítimas (González Rus, 2024: p. 929). La mera adquisición, posesión, utilización, conversión o transmisión de tales bienes debería conformar un acto neutro, que no colma las exigencias de tipicidad del delito que se analiza[7].

Pese a que el blanqueo de capitales es un fenómeno que supone laxismos técnico-jurídicos y distintas acepciones en función de la jurisdicción de que se trate (Souto, 2021: p. 5[8]), hay consenso a nivel global en considerarlo un delito[9], pues es una amenaza para el sistema financiero internacional (Zeldin, 1994: p. 221)[10] y a esa escala hay que darle respuesta. Según

[6] Es también la apreciación de Morillas Cueva (2013: p. 78). El reconocido penalista señala que el bien jurídico protegido debe ser el orden socioeconómico y, a partir de allí, puede concretarse en el mercado, la libre competencia, entre otros.

[7] Considera Alldridge (2001: p. 289) que asimilar el delito de blanqueo de capitales como conexo al delito previo y no como un delito autónomo impide proyectar su importancia y el daño que causa.

[8] El autor entiende que la expresión "blanqueo de capitales" entraña un término laxo y otro demasiado preciso. Además, no se conoce igual a este fenómeno en todas las regiones del mundo.

[9] Diversos instrumentos internacionales han promovido la importancia de tipificar el blanqueo de capitales en cada país. Por ejemplo, la Convención de Viena de 1988 exhortó en el art. 1. b) i) a castigar penalmente "la conversión o la transferencia de bienes a sabiendas de que tales bienes proceden de alguno o algunos de los delitos tipificados […], con objeto de ocultar o encubrir el origen ilícito de los bienes o de ayudar a cualquier persona que participe en la comisión de tal delito o delitos a eludir las consecuencias jurídicas de sus acciones". Estas indicaciones internacionales han fomentado la armonización y cooperación a nivel internacional, a la hora de entender y tratar este supuesto.

[10] Asimismo, señala Unger (2007: p. 14); que no solo pequeñas islas —por ejemplo, los conocidos "paraísos fiscales"— blanquean dinero, sino que lo hacen en mayor medida las economías ricas y desarrolladas.

datos ofrecidos por el Consejo Europeo y el Consejo de la UE[11], entre 715000 millones y 1,87 billones de euros del PIB mundial se blanquean anualmente. En el espacio de la Unión se estiman entre 117000 y 210000 millones de euros involucrados en actividades sospechosas de blanqueo. Años atrás, la mayor preocupación en torno al blanqueo ilícito de bienes era el uso de dinero en efectivo y el tráfico de drogas (Schneider & Windischbauer, 2010: pp. 4 y 5), lo cual ha ido ampliándose paulatinamente. Las nuevas tecnologías han hecho que el blanqueo de capitales sea más complejo y global, lo cual plantea desafíos significativos para la regulación y el cumplimiento de la ley, exigiendo una constante adaptación y el uso de tecnologías avanzadas para combatir este crimen transnacional[12]. Las transacciones en línea, a través de distintas plataformas, permite a los delincuentes movilizar activos y dinero a cualquier parte del mundo en segundos (Guidara, 2022: p. 37). Por si eso fuera poco, el grado de anonimato que brindan las criptomonedas, su uso accesible y sencillo para cualquiera y su divisibilidad (Manninen, 2023: pp. 10 y 12), las hacen potencialmente útiles en este contexto delincuencial. Y es perfectamente posible la colocación de los bienes ilícitos en el orden socioeconómico —requisito del blanqueo de capitales—, pues los delincuentes pueden cambiar los activos virtuales por divisas o al revés.

El Código Penal español, en atención a las exigencias internacionales y la magnitud del fenómeno que supone el blanqueo de capitales, procede a tipificarlo en el art. 301.1. Los verbos rectores del tipo son adquirir, poseer, utilizar, convertir o transmitir bienes, a sabiendas de su procedencia delictiva[13] o realizar "cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a

[11] Recurso electrónico disponible en el siguiente enlace: https://www.consilium.europa.eu/es/infographics/anti-money-laundering/#:~:text=El%20blanqueo%20de%20capitales%20en,2%20%25%20y%20el%205%20%25). Consultado por última vez el día 31 de julio de 2026.

[12] Es necesario recordar que el blanqueo de capitales está altamente vinculado con el crimen organizado. Sin embargo, hay que tener también en cuenta que la delincuencia organizada no persigue siempre la obtención de ganancias como objetivo prioritario, sino el cumplimiento de compromisos éticos y la imposición de creencias personales. Al respecto, *vid.* Levi & Soudjin (2020: 5). En Alemania se ha planteado si, en vez de centrar la lucha contra la criminalidad organizada en la prevención del blanqueo, lo conveniente es perseguir con ahínco los hechos previos. También *vid.* Manso Porto, T. (2011) «El blanqueo de capitales entre la dogmática y la Política criminal internacional: Resultados desde una perspectiva de Derecho comparado». *Estudios Penales y Criminológicos,* vol. 41, p. 316.

[13] No habla de un número limitado de delitos previos, sino que se trata de una forma gramatical que da lugar a una "interpretación extensiva y analógica de la norma por parte de los Tribunales (Carballo, 2023: s/p).

eludir las consecuencias legales de sus actos"[14]. La STS 8701/2012 (FJ 27)[15] destaca que adquirir, convertir o transmitir bienes son "comportamientos genuinos de blanqueo". El resto de conductas descritas —incluyendo una fórmula abierta que da cabida a "cualquier otro acto" que pretenda encubrir los fondos ilícitos— han sido altamente cuestionadas por tratarse de un *totum revolutum* que recoge acciones sin orden (De Mosteyrín Sampalo, 2016: p. 392) y, por tanto, tener graves problemas de claridad y esquematización (Aránguez Sánchez, 2020: p. 685). Esto ha dado lugar también a un acalorado debate sobre si es punible el autoblanqueo o no, cuya solución puede tener dos vías: si se trata de un acto copenado del delito antecedente y, por tanto, no punible cuando el que blanquea es también el autor de aquel; o si se trata de un comportamiento que da lugar a un injusto autónomo (Olmedo Cardenete, 2024: p. 930). Con todo, para estar ante el delito de blanqueo tienen que darse una relación clara entre el flujo de dinero manejado y la cuota que se ha defraudado (STS 277/2018, FJ 44).

Cuando el tipo penal habla de bienes con procedencia ilícita, no cabe duda de que cobija a las criptomonedas, tanto si se han obtenido directamente ellas con el delito previo, como si se han adquirido *a posteriori* con las divisas u otros activos generados por la actividad criminal. La pretensión es evitar el blanqueo de "cualquier tipo de participación delictiva previa" (Molina Mansilla, 2007). Por eso, no ha sido necesario incluir expresamente a los activos virtuales en la tipificación del delito, sino que se ha considerado aplicable el existente en todo aquello que sea posible, siendo esta la línea de las Directivas europeas (Nieto Martín & García Moreno, 2021: pp. 4 y 5) y del GAFI[16]. Pese a que, como se ha avanzado, el TS ha intentado acotar a nivel interpretativo el delito de blanqueo, por su ambigüedad y extensión, la Abogacía Española (2022: s/p) reconoce que seguramente están conociendo ya causas de este tipo. Esto confirma que no ha sido necesario reformar el Código Penal para incluir expresamente las criptomonedas, ya que el marco legal vigente tiene la flexibilidad suficiente para cubrir este tipo de activos[17].

[14] También constituye delito la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos, a sabiendas de su origen ilícito (art. 301.2 CP).

[15] La resolución indica que por adquisición hay que entender la incorporación de bienes al patrimonio propio, a título oneroso o gratuito; por conversión, la transformación de bienes en otros distintos; y por transmisión, la extracción de bienes de su patrimonio para integrarlo en el de alguien más.

[16] La nota interpretativa de la Recomendación 15 del GAFI expresa que los activos virtuales deben ser considerados como bienes, productos, fondos u otros activos.

[17] Además, comenta Matallín Evangelio (2018: p. 281) que la extensión del art. 301 CP se aprecia también en la indeterminación de los bienes que se originan en una actividad delictiva previa. Similar a esta postura, Díaz-Maroto y Villarejo (2017: p. 149)

Tampoco tendría sentido hacer una interpretación restrictiva de la redacción del delito que excluya a los criptoactivos, ni por cuestiones gramaticales ni mucho menos teleológicas.

El Código Penal español admite, en el art. 302.2, la posibilidad de que personas jurídicas sean responsables penalmente por el delito de blanqueo de capitales. Es un aspecto contenido en la Recomendación 3 del GAFI y obedece a cuestiones de política criminal, por la frecuente instrumentalización de las personas jurídicas en sede de blanqueo de capitales (González Quinzán, 2023: p. 422). Lascuraín Sánchez (2018: pp. 513 y 514) apunta que a la persona jurídica no se le castiga por blanquear, sino por permitir que sus administradores, directivos o empleados blanqueen en beneficio de aquella. La comisión del delito de blanqueo de capitales por parte de una persona jurídica puede producirse porque sus administradores o directivos no han cumplido sus obligaciones de control o por colaborar activamente con las actividades de blanqueo; o bien porque tales sujetos no han supervisado adecuadamente la ejecución de las obligaciones de control de los empleados (Fernández Teruelo, 2019: pp. 18-22). En el caso de las criptomonedas, los prestadores de servicios de criptoactivos no son las únicas personas jurídicas alcanzadas por las disposiciones penales, aunque tienen un rol especialmente regulado debido a su proximidad al manejo directo de activos digitales. Otras entidades que pueden resultar responsables son, por ejemplo, desarrolladores de *software*, entidades comerciales que acepten pagos en criptomonedas sin implementar mecanismos de prevención o empresas consultoras, auditoras y asesoras legales, aunque se espere mayor diligencia por parte de los sujetos obligados por la normativa antiblanqueo. Esto refuerza la importancia de implementar políticas estrictas de *compliance* en todos los sectores que interactúan directa o indirectamente con activos digitales.

II. FASES DEL BLANQUEO DE CAPITALES Y SU RECONOCIMIENTO CUANDO MEDIAN CRIPTOMONEDAS

1. *Fase de colocación*

Para que los delincuentes puedan blanquear beneficios ilícitos, siguen una serie de pasos que la doctrina, la jurisprudencia y los organismos internacionales[18] han agrupado principalmente en tres etapas: la colocación, la

considera que el Legislador ha optado por una fórmula típica amplia que evita señalar medios comisivos específicos, sino que se centra en determinados ánimos del que comete el delito.

[18] La propuesta tripartita que se analizará a continuación fue especialmente impulsada por el GAFI; el máximo organismo internacional para la lucha contra el blanqueo de capitales. Lo planteó inicialmente en el informe: "Tipología del blanqueo de capitales" en

ocultación y la integración de los activos. En cada una de ellas se producen diversas actividades o técnicas y pueden intervenir varios sujetos (Jiménez García, 2016: p. 219). La primera fase, la colocación, consiste en la introducción de los capitales o efectos en el mercado, con la finalidad de desvincularlo del delito que les dio origen (Delgado Sancho, 2023: p. 17). Frecuentemente, esto se logra depositando en diversas cuentas bancarias pequeñas sumas de dinero u obteniendo determinados instrumentos financieros con ellas, en vez de movilizar grandes cantidades en una misma transacción. El objetivo de esta fase es evitar sospechas, pues hay un alto riesgo de ser descubierto (Arman, & Nendi, 2023: p. 358); por lo que es un período crítico en la comisión delictiva. También es útil en este contexto crear empresas "tapadera" que, a su vez, pueden estar relacionadas con organizaciones mafiosas o ser subcontratados a cambio de una comisión (Sánchez Seco, 2013: p. 191) y valerse de otras herramientas, como agentes de seguros, de viajes, inmobiliarios, para convertir los bienes ilícitos (Amrani, 2012: pp. 26 y 27).

Las criptomonedas allanan en gran medida la fase de colocación. Los delincuentes pueden cambiar los efectos obtenidos con la actividad criminal por tales activos, caracterizados, como se sabe, por su opacidad. Generalmente, cuando el blanqueo en la fase de colocación se realiza a través de cuentas bancarias, se solicita a estas entidades información sobre el movimiento realizado. Con las criptomonedas este filtro se diluye, pues no dependen de la verificación ni seguimiento de los bancos centrales y otras autoridades gubernamentales[19]. Será necesario que las autoridades requieran de la ayuda y soporte que pueden suministrar las casas de cambio y otros proveedores de servicios cripto, que están más cerca de las operaciones cotidianas de los usuarios y pueden implementar controles efectivos. Por eso, las actuales medidas antiblanqueo se orientan a que las plataformas mediadoras, los proveedores de servicios de activos virtuales, requieran información obligatoria de sus clientes (Jabotinsky & Lavi, 2022: p. 585). En caso de presunto delito, estos datos pueden ser suministrados a los funcionarios y encargados de administrar justicia para facilitar las labores de rastreo.

Otra razón por la que las criptomonedas mejoran la perpetración del blanqueo, y concretamente la primera fase, es que su divisibilidad permite el intercambio de bienes y capitales en múltiples pequeñas transacciones. Los

1990. Por eso, Van Koningsveld (2013: pp. 4 y 5) cuestiona si este esquema sigue siendo útil en la práctica actual, habiendo ampliado el blanqueo de capitales a muchos otros delitos y alejándolo de la vinculación monótona que tenía con el tráfico de drogas.

[19] Afirman Kim, et al. (2021) que los Gobiernos no pueden monitorear directamente todas las transacciones realizadas con criptomonedas, verificando minuciosamente cada movimiento y sus partes involucradas.

delincuentes pueden realizar una técnica conocida como *smurfing*, que consiste en dividir grandes cantidades de dinero[20]; en este caso, en transacciones menores a mil euros para evitar la notificación obligatoria[21]. Aunque este límite cuantitativo a la movilización libre de criptomonedas es útil para prevenir el blanqueo —obstaculiza, en definitiva el intercambio de grandes sumas de dinero, pues los criminales necesitarán hacer muchas transacciones—, no es infalible. La movilización de activos virtuales es muy rápida y sin engorrosos trámites, requerimientos o autorizaciones, como ocurre con el sistema financiero tradicional. Además, conforme se vayan aceptando como medio de pago con mayor amplitud, más sencillo será diversificar los bienes ilícitos y transformarlos (Albrecht, et al., 2019: p. 213). El *smurfing* no es una técnica nueva, pero sí perfeccionada por las criptomonedas. Ha devenido como un problema global (Forgang, 2019: p. 14) por diversas causas:

– La complejidad que supone rastrear movimientos que involucran a múltiples personas e instituciones financieras. El término *smurfing* viene de *smurf*, que significa "pitufo", haciendo alusión a la imagen de los pitufos, que son pequeños, numerosos y difíciles de identificar cuando actúan en grupo.
– La falta de denuncia de las entidades encargadas de hacerlo por no reconocer *a priori* que se trata de fondos ilícitos o de transacciones sospechosas. De tal forma que, para mejorar la detección de fondos ilícitos, se necesita fortalecer la capacitación y el análisis de riesgos en las entidades financieras, y utilizar tecnologías avanzadas de monitoreo que identifiquen patrones sospechosos de manera automática.
– La constante actualización de las técnicas empleadas por los delincuentes.
– Los limitados recursos de los agentes que hacen cumplir la Ley y que condiciona su capacidad para investigar, detectar y prevenir el blanqueo de capitales.

Pese a lo anterior, hay estudios de ciencias técnicas que exponen algunas soluciones. Por ejemplo, Koelbing et al. (2024: pp. 6 y ss.[22]) proponen la

[20] Mooij (2024) define dos modalidades de *smurfing*: introducir pequeñas cantidades de activos de diversas fuentes a través de una misma institución en varios puntos de venta o hacerlo a través de varias instituciones en un punto de venta único. Además, la autora señala que el *smurfing* es una técnica muy eficiente para lavar activos en el metaverso, pues la economía que propicia se basa, en gran medida, en las criptomonedas.

[21] La normativa europea y las recomendaciones internacionales imponen un límite de mil euros a las transferencias con criptoactivos. Movimientos con una cuantía superior deben ser notificados por los proveedores de servicios para combatir el blanqueo de capitales y la financiación del terrorismo.

[22] Los autores reconocen que su experimento puede no ser suficiente para identificar todas las propiedades del blanqueo de capitales en el mundo real, aunque lo consideran un

modelización de patrones de transacciones múltiples sujetas al umbral cuantitativo de la normativa antiblanqueo, haciendo particiones de los movimientos realizados con un sistema de álgebra computacional y modelando el comportamiento transaccional ilícito, conocido como *smurfing*. Otro gran aporte es el de Shadrooh y Nørvåg (2024: pp. 7466 y ss.[23]), quienes han desarrollado SMoTeF, un proceso de varias etapas basado en dos algoritmos de análisis de gráficos que evolucionan en el tiempo para identificar casos de *smurfing*. El marco creado permite contrastar redes de este tipo fraudulentas y no fraudulentas, de acuerdo con la densidad del flujo de dinero, flujos temporales máximos y restricciones de orden temporal. Otras proposiciones persiguen la utilización de bases de datos gráficas y la minería de tales datos para trazar el flujo monetario hasta detectar la cuenta destinataria final, que sería la del criminal (El-Banna, et al., 2020); y/o de uniones simples a bases de datos para comparar y clasificar la información de los grafos estudiados (Starnini, et al., 2021). El patrón común de todas estas ideas es el uso de técnicas avanzadas de análisis de datos y modelado de patrones para detectar el *smurfing*. En este sentido, es relevante el tratamiento de grafos y la minería de datos.

2. *Fase de estratificación*

La segunda fase del blanqueo de capitales es el ocultamiento o estratificación de los bienes. El objetivo de esta etapa es ocultar el rastro del origen de los fondos, a partir de la ejecución de transacciones financieras legales. Esto suele conseguirse con transferencias a una cuenta en el extranjero (Albrecht, et al., 2019: p. 211), conversión a otros instrumentos menos rastreables, facturas y demandas judiciales falsas (Thommandru, 2023), inversión en bienes raíces y otros negocios legítimos o la creación de empresas "fantasma" (Scott, 1995: p. 1), etc. Mucho más eficiente será el esquema de lavado si el criminal mueve sus fondos a cuentas de distintas jurisdicciones a través de un grupo de empresas (Yazid bin Zul Kepli & Adeniyi Nasir, 2016: p. 33). La creación de capas artificiales y complejas de propietarios hace que los fondos

avance. También sería necesario determinar en qué medida los datos obtenidos por la aplicación de este método podrían ser válidos en un proceso judicial de blanqueo o si constituirían un indicio claro de este delito. El modelo aplicado que se expone deriva de un primer estudio de los mismos autores y otro; a saber, Gran, et al. (2023).

[23] Los investigadores identifican las siguientes limitaciones en su propuesta: puede ser complicado abordar patrones de *smurf* en cadenas donde intervienen varios intermediarios, el mantenimiento del proceso requiere el conocimiento y experiencia de profesionales familiarizados con el dominio de aplicación concreto de SMoTeF y la posibilidad de falsos positivos. El primero y el último de los obstáculos mencionados son prioridades en los trabajos futuros de los autores citados.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

tomen caminos y formas que son de difícil distinción al final de esta fase (AML UAE, 2023: p. 5). Las criptomonedas permiten la creación de rutas financieras complejas, al permitir la transferencia rápida de fondos a múltiples *wallets*, en cualquier lugar del mundo, disgregándolos en jurisdicciones dispares y hasta con bajo grado de cooperación.

Un método común para el ocultamiento de bienes y activos con criptomonedas es el salto de cadena o *chain hopping* (Prendi, Borakaj & Prendi, 2023: p. 86), que consiste en convertir una criptomoneda en otra de forma repetida con sucesiones muy rápidas para que pase por diferentes *blockchains*. ELLIPTIC (2022: p. 8) prevé que su uso será cada vez más frecuente por los criminales, pues dificulta el rastreo de fondos y suelen cristalizarse con la adquisición de criptomonedas de privacidad en jurisdicciones con regulaciones menos exigentes en materia de blanqueo de capitales. Estos intercambios podrían hacerse a través de una DEX, por ejemplo. El GAFI (2023: p. 39) considera que esto obliga a las autoridades a familiarizarse con las capacidades de análisis y monitoreo de las cadenas de bloques a través de sistemas inteligentes y herramientas complementarias para estos métodos más específicos[24]. Más crítico es el supuesto si el delincuente se vale de *cold wallets*, ya que al no estar conectadas a la red son menos rastreables.

Otra herramienta útil para la estratificación de los beneficios obtenidos ilícitamente son los *mixers*. Estos servicios intercambian los flujos de muchos propietarios para reducir la transparencia de las transacciones con activos virtuales. Para el GAFI (2019: p. 36) se trata de un área de riesgo a la que se debe dar prioridad, pues ofusca aún más los movimientos y socavan la capacidad de los prestadores de servicios de activos virtuales —sujetos obligados por la normativa antiblanqueo— para implementar medidas de KYC y debida diligencia. Como los mezcladores vinculan transacciones desde una misma dirección pública y las envía de forma simultánea a otras varias simuladas, hay una dispersión de la trazabilidad (Cevallos Pachacama, 2024: p. 15) que complica la identificación del autor o autores potenciales del delito. Las soluciones propuestas están nuevamente orientadas hacia el análisis avanzado de Blockchain con herramientas como *Chainalysis*, *Elliptic* o

[24] Un caso conocido es de *Baller Ape*, un *token* no fungible que fue propuesto por un ciudadano vietnamita como proyecto de inversión. Al poco tiempo, los impulsores del mismo, según la acusación, ejecutaron una "tirada de alfombra" o *rug pull*. La misma acusación indica que estos individuos utilizaron "saltos de cadena" para ocultar el rastro de los fondos presuntamente estafados a los inversores, que ascienden a 2,6 millones de dólares. Este caso está siendo sustanciado ante el Departamento de Justicia del Distrito Central de California desde 2022 (expediente judicial: 2:22-cr-273). *Vid.* Departamento Del Tesoro De Los Estados Unidos (2023: pp. 22 y 23). No es un caso propiamente de criptomonedas, sino de NFT, pero es un antecedente que ilustra la complejidad y forma de perpetración que puede presentar el blanqueo de capitales en el contexto cripto.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

CipherTrace, que cuentan con técnicas avanzadas para detectar patrones en las transacciones que atraviesan *mixers*. También se pueden aplicar heurísticas para agrupar direcciones que podrían estar controladas por la misma entidad, especialmente si se comete algún error operacional durante el uso de los mezcladores. Y, aunque no sea una tarea sencilla —de hecho, prácticamente imposible sin la intervención de agencias internacionales—, se podrían intervenir los propios servicios de *mixer* e incautar los activos que están bajo su poder.

Ejemplo de lo último es el caso de *ChipMixer*, un mezclador de criptomonedas sin licencia cuya infraestructura fue desmantelada por un grupo de autoridades nacionales con el apoyo de EUROPOL. Con la operación, se recuperaron casi dos mil BTC y obtuvieron datos para seguir investigando a los criminales que se valieron de dicho servicio (EUROPOL, 2023)[25]. No hay muchas probabilidades de éxito si lo que se pretende es suprimir las plataformas de *mixing*[26], pero sí de intervenirlas y trabajar con la información que contienen. Por eso, EEUU ha emitido una Declaración con la que indica expresamente el sometimiento de los mezcladores a la normativa de prevención de blanqueo de capitales y financiación del terrorismo (Del Monaco, 2020: pp. 13 y 14), como un prestador de servicios de criptoactivos más. Sin embargo, las exigencias que le son propias a estos sujetos según la normativa antiblanqueo —el deber de KYC o la debida diligencia, por ejemplo— colisiona de base con la finalidad de los *mixers*, que es aumentar la privacidad y reducir la trazabilidad (Mooij, 2024: pp. 71 y 72).

Enviar fondos y difuminarlos en el extranjero es totalmente accesible con las criptomonedas. Esta característica, que supone un serio riesgo para el blanqueo de capitales, se ve agudizada con los centros financieros *offshore,* definidos por Subashi (2024: pp. 59 y 60) como "jurisdicciones que tienen un número relativamente grande de instituciones financieras dedicadas principalmente a negocios con no residentes; sistemas financieros con activos y pasivos externos desproporcionados en relación con la intermediación financiera interna diseñada para financiar las economías nacionales; y, más popularmente, centros que ofrecen algunos o todos los siguientes servicios:

[25] Otro supuesto conocido es el de *bestmixer.io*, mezclador que fue desmantelado por el Equipo Cibernético Avanzado Financiero del Servicio de Investigación e Información Fiscal de Países Bajos, el Equipo de Intrusión Digital de la policía del mismo país, EUROPOL y autoridades de Luxemburgo, Francia y Letonia. La cooperación dio lugar a la confiscación de seis servidores que estaban en funcionamiento.

[26] Por ejemplo, en 2022 el Departamento del Tesoro de EEUU determinó una serie de sanciones contra el mezclador *Tornado Cash*, incluyendo su bloqueo. Sin embargo, como se trata de una entidad descentralizada desplegada en una plataforma resistente a la censura, es muy difícil eliminarlo de la red. Al respecto, resulta relevante el estudio de Brownworth, A. et al. (2024: pp. 2, 3, 11-13).

impuestos bajos o nulos; regulación financiera moderada o ligera; secreto bancario y anonimato". Se ha advertido que estos centros juegan un papel crucial para ocultar actividades ilegales, la identidad de los criminales y la propiedad de los activos involucrados (Unger, 2017: p. 7). Aquellos ofrecen un refugio seguro para los criminales (Hellvig & Blanaru, 2023: p. 92), pero cuanto más se integren criptomonedas en estos entornos *offshore*, más difícil será para las autoridades desmantelar las redes criminales y aplicar sanciones efectivas.

Dos aspectos más empleados para la estratificación de bienes y efectos ilícitos son advertidos por Hinojal Fraile (2023: p. 228): a. Los videojuegos en línea, ofreciendo productos digitales dentro de los juegos que permiten la ejecución del blanqueo; y b. el uso de criptocajeros. Ambos mecanismos parecen inofensivos pero tienen aptitudes amplias para la perpetración del delito analizado. En el caso de los juegos en línea, no obstante, no suelen ser útiles para el blanqueo de grandes volúmenes de ganancias (Monteiro Lima & Márcio, 2021: p. 11), y en el de los cajeros de activos virtuales, su uso aún no está lo suficientemente extendido para ser una herramienta principal en el blanqueo de dinero, ya que su accesibilidad para los blanqueadores sigue siendo limitada. Ante el riesgo de los segundos, el regulador financiero central de Alemania realizó una redada por todos los cajeros de criptoactivos del país que no tenían permiso para funcionar, confiscando las máquinas e incautando los activos con los que operaba[27]. En general, el Reglamento (UE) 2023/1113 indica que este tipo de cajeros deben acomodarse a las exigencias en materia de blanqueo, al estar comprendidos dentro de su ámbito de aplicación. Esto incluye medidas de mantenimiento, de seguridad y de supervisión por parte de sus operadores (Sanz-Bas, et al., 2021: p. 14).

3. *Fase de integración*

La tercera y última fase asociada al blanqueo de capitales es la integración de los ingresos ilegales en el sistema financiero legítimo. Lógicamente, es el culmen del delito de blanqueo, aunque no es necesario llegar a su materialización para que se entienda consumado, vista la amplitud de sus conductas típicas. La estratificación y la integración son las dos fases con mayor grado de interés regulatorio (Jabotinsky & Lavi, 2022: pp. 540 y 541). Al llegar a este punto, los criminales son libres para utilizar los fondos de diversas maneras, pudiendo perseguir fines legítimos o nuevamente ilícitos (Amrani,

[27] Puede consultarse la noticia y datos de la operación realizada por el BaFin, la policía y el Bundesbank alemán en el siguiente enlace: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2024/pm_2024_08_20_Krypto_Automaten.html. Consultado por última vez el día 31 de julio de 2026.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

2012: p. 28[28]). La integración convencional resulta de inversiones, préstamos, compra y venta de productos. En el espacio virtual cualquiera de estos procesos se simplifica, con menos riesgos para el delincuente (Arman & Nendi, 2023: p. 350). La intercambiabilidad de las criptomonedas y su estrecha interacción con el sistema financiero tradicional las convierte en un terreno especialmente fértil para liquidar el proceso de blanqueo. Pero no hay que olvidar, como bien resalta Navarro Cardoso (2019: pp. 30-32), que la monetización —es decir, la conversión de activos virtuales a dinero de curso legal— es innecesaria, dada la suerte de que los delincuentes pueden optar por la "tokenización"; a saber, la transformación en otros criptoactivos.

El TS[29] resalta que el hilo conductor de las tres fases consideradas es la clandestinidad y el diseño de una arquitectura con apariencia legal. La globalización de las actividades de blanqueo, la profesionalización en el ejercicio del delito y la complejidad de los métodos empleados facilitan y refuerzan esta apariencia de legalidad (Blanco Cordero, 2021: pp. 56-61). Estos factores han llevado a un aumento en la sofisticación de las operaciones de blanqueo, lo que complica la detección y persecución por parte de las autoridades (Del Monaco, 2020: p. 226). En vista de este cambio de paradigma, se ha señalado la imposibilidad de que el modelo de tres etapas del blanqueo de capitales baste para explicar el fenómeno actual[30]. Sin embargo, la secuencia de pasos tradicionales es lo suficientemente genérica como para reconocer la dualidad del entorno digital y físico y abordar las herramientas específicas que ofrece el mundo cripto.

III. DELITOS RELACIONADOS CON EL BLANQUEO DE CAPITALES Y CRIPTOMONEDAS

1. *La receptación*

La receptación es un delito autónomo tipificado en el Código Penal español en el art. 298, donde se castiga la ayuda a los responsables de un delito del que no se es parte, ni como autor ni como cómplice, a que se beneficien

[28] El autor señala la posibilidad de que los fondos blanqueados se dirijan a la financiación del terrorismo. Como afirma Murphy (2024: p. 3), en la tercera etapa los movimientos son menos sospechosos. Por tanto, la clave del éxito en la prevención del blanqueo de capitales es identificar el crimen en estadios previos.

[29] STS 156/2011, 21 de Marzo de 2011.

[30] Por ejemplo, Van Koningsveld (2013: pp. 7 y 8) propone un modelo de cuatro etapas, donde se mantienen las dos primeras, pero la tercera pasa a ser la justificación del dinero que se pretende blanquear y su inversión en esquemas lícitos. Relacionado con lo anterior, Casella (2018) explora las razones por las que el modelo de tres fases se queda obsoleto, especialmente cuando se trata de fondos que se negocian por vía electrónica.

de los efectos del mismo; o su recepción, adquisición u ocultamiento[31]. Al igual que en el blanqueo de capitales, la tipificación exige la ocurrencia de un delito previo. Pero, a diferencia de aquel, la receptación solo limita su *ratio* de aplicación a los casos en que la conducta criminal previa sea contra el patrimonio o el orden socioeconómico. El comportamiento ilícito que se analiza requiere, en palabras de Reinoso Martínez (2020: p. 112), un elemento tendencial —el ánimo de lucro— y otro subjetivo —que el receptador tenga conocimiento de la comisión del delito previo—. A estos, añade De Vicente (2024: ep. 517), un elemento negativo, basado en la circunstancia de que el autor de este delito, no puede serlo del anterior. Por ello, puede darse el autoblanqueo, pero no así en el caso de la receptación. En el segundo se pena que un tercero se beneficie de la rentabilidad del delito o ayude a su autor a hacerlo (Pérez Gómez, 2015); de ahí que se exija el elemento mencionado. Por ello, es recognoscible que se trata de un delito pluriofensivo, en el que se lesionan el patrimonio del titular de la cosa, en su caso; el orden socioeconómico y la Administración de Justicia. Su fundamento se reconoce en la STS 139/2009 (FJ 4): perpetuar la ilicitud previa y estimular la comisión de los delitos contra el patrimonio y el orden socio-económico.

El blanqueo de capitales y la receptación tienen notorias diferencias[32], pero también aspectos de fricción[33]. Ambos delitos están relacionados con la gestión o efectos de procedencia ilícita, por lo que son modalidades postdelictuales (Mendoza Llamacponcca, 2014: p. 326). Por eso, no es extraño que puedan dar lugar a un concurso de leyes que, de acuerdo con el criterio de Aránguez

[31] Las conductas típicas son descritas por Vázquez Iruzubieta (2015: pp. 694 y ss.). La ayuda —que constituye un delito de consumación anticipada— debe consistir en favorecer que los responsables del delito previo se aprovechen de los efectos, sin importar si esta es del todo necesaria para la producción del resultado; la recepción se debe entender como depósito o guarda o alguna contribución para dificultar la persecución del delito, pero se excluye cualquier negocio jurídico gratuito por el ánimo de lucro; la adquisición debe ser para uso previo en el tipo básico, pues si es para traficar daría lugar a la agravante específica del apartado segundo; la ocultación alude a la acción de esconder o disimular los bienes receptados.

[32] La STS 408/2015, 8 de Julio de 2015, FJ 2; identifica las siguientes diferencias: "1. Mientras en la receptación y en el encubrimiento el Legislador excluye explícitamente a los partícipes del delito previo, esta exclusión no se ha incorporado nunca a la descripción del tipo del blanqueo […] 2. Pese a la proximidad del blanqueo con la receptación, la mayor gravedad del blanqueo para el Legislador es obvia dada la entidad de las penas que respectivamente les conminan. 3. La mayor autonomía del blanqueo de capitales frente al delito previo, respecto de la receptación y el encubrimiento, resulta de toda ausencia limitativa de la pena del blanqueo a la del delito previo, como se establece para el encubrimiento y la receptación". También *vid.* la STS 809/2014 de 26 de noviembre.

[33] Basta con ver la rúbrica del Capítulo XIV donde se insertan ambos delitos: "De la receptación y el blanqueo de capitales".

© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

Sánchez (2000: p. 364)[34], debe resolverse a favor de la receptación por tratarse de una ley especial y más restringida que el blanqueo. Esto es, además, lo que consagra el art. 8.1 CP: "El precepto especial se aplicará con preferencia al general". Solo en defecto de otros criterios, se aplicaría el precepto penal más grave y se excluiría el que fije una pena menor (art. 8.4). Recalca el TS[35] que hay que reservar un espacio propio para el delito de receptación, en vista de "la imparable expansión del delito de blanqueo de capitales". Se trata de una cuestión magna en el contexto cripto, pues determinar cuándo estamos ante una figura delictiva y cuándo en la otra puede ser embrollado.

Si un prestador de servicios de criptomonedas, persiguiendo un ánimo de lucro, ayuda a delincuentes a ocultar o aprovecharse de los efectos ilícitos que se generaron con la producción de un comportamiento criminal contra el patrimonio y/o el orden socioeconómico —hurtos, robos, extorsiones, usurpaciones, modelos defraudatorios, insolvencia punible, delitos societarios…—, podría tratarse de un delito de receptación y no necesariamente de blanqueo de capitales. Estos sujetos también pueden lucrarse con la custodia de las criptomonedas y su consecuente disimulo. El mismo caso puede ocurrir con los servidores de *mixing*, siempre que sean conscientes de que los clientes/usuarios han cometido el delito previo y les están ayudando a "alcanzar el agotamiento material de sus propósitos o a conseguir burlar la acción de la justicia" (STS 67/2006, FJ 13). En los mencionados supuestos, se trataría de una receptación profesional, al implicar establecimientos o locales comerciales. La clave para diferenciar que la conducta de los sujetos expuestos se subsume en la receptación parece ser la presencia del ánimo de lucro y no la integración de los bienes ilícitos en el sistema económico legal. Este elemento típico no se exige ni en el blanqueo ni en el delito de encubrimiento, aunque puede darse. El ánimo de lucro puede ser más sencillo de probar en el caso de personas jurídicas que están debidamente constituidas y que inobservan adrede las exigencias legales de *compliance* en materia cripto. Pero no será asequible si se receptan bienes a través del intercambio en plataformas P2P de uso privado, DEX o *traders* que actúan como custodios informales. La comprobación de los elementos típicos en estos casos puede hacer más complicada la atribución de responsabilidad penal.

[34] Por su parte, Lascuraín Sánchez (2018: pp. 520 y 521) agrega una figura más a la ecuación: el encubrimiento tipificado en el art. 451 CP. En vista de ello, concluye lo que sigue: "La defectuosa técnica legislativa hace que cuando en una conducta se den los rasgos de la receptación y el blanqueo o el encubrimiento y el blanqueo parece que deban aplicarse los primeros, más específicos porque se refieren a un ocultación o encubrimiento más específicos en cuanto al tipo de bienes o al tipo de ánimo, lo que parece frustrar la voluntad agravatoria que guía la tipificación del blanqueo".

[35] STS 408/2015, 8 de Julio de 2015, FJ 1.

Todos estos estorbos de interpretación y aplicación de figuras delictivas tan afines suelen hacer que la receptación quede rezagada a un segundo plano, especialmente al verse embebido por el blanqueo de capitales. Dicho esto, en el seno de organizaciones criminales dedicadas a la delincuencia con criptomonedas, puede perfectamente darse el caso de que se produzcan ambas modalidades típicas, por la interacción de diversas personas con roles distintos. En abril de 2024, por ejemplo, la operación "Vallota" de la Guardia Civil española acabó desmantelando una organización criminal dedicada al tráfico de vehículos de alta gama robados en España y Suecia para venderlos en otros países. Como resultado, 21 personas han sido detenidas por: delitos de pertenencia a organización criminal, tráfico ilícito internacional de vehículos, blanqueo de capitales, estafa, falsedad documental, tenencia ilícita de armas, delito de daños, usurpación de identidad y receptación (Ministerio del Interior, 2024).

2. *El delito fiscal*

El art. 305.1 CP contiene el tipo básico de lo que se conoce como delito fiscal. Se castiga por vía penal al que defraude a la Hacienda Pública, eludiendo el pago de tributos, obteniendo devoluciones indebidas o disfrutando de beneficios fiscales que no le correspondan. Cámara Barroso (2016: p. 5) aclara que es necesaria la producción de cierto engaño por parte del sujeto activo. Este ardid tiene particularidades propias, frente a otros engaños —como el propio de la estafa—, no siendo necesaria una liquidación *mise en scène* de los tributos (Barrera & Hessdörfer Rozen, 2012: p. 20)[36]. La acción típica puede producirse alegando gastos que no se han producido, no aportar conscientemente datos fiscales obligatorios o necesarios a las autoridades o facilitar información falsa a las mismas, presentar declaraciones falsas, entre otros (Kublen, 2015: p. 28). En general, para comprobar la producción del perjuicio hay que verificar la existencia de falsedad, por las exigencias del tipo objetivo (De la Mata Barranco, 2016: p. 15). Otro aspecto relevante del delito es la delimitación cuantitativa del daño para que se entienda cometido el delito. De acuerdo con el mismo artículo citado, la cuantía de la cuota defraudada, el importe no ingresado de las retenciones o ingresos a cuenta o de las devoluciones o beneficios fiscales indebidamente obtenidos o disfrutados debe exceder de 120.000 euros, para estar ante el delito básico de fraude fiscal.

El Legislador también incluye tipos cualificados, contenidos en el art. 305 bis CP. Es crucial destacar que la responsabilidad fiscal es importante para mantener la calidad de los servicios público y de las prestaciones sociales, lo cual repercute

[36] De hecho, el propio precepto indica que "la mera presentación de declaraciones o autoliquidaciones no excluye la defraudación, cuando ésta se acredite por otros hechos" (art. 305.1 CP).

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

en gran medida en la calidad de vida de las personas. Por eso, Martiñón (2012, pp. 173 y 174) lo define como "uno de los valores básicos sobre los que se articula la convivencia social en las sociedades democráticas actuales".

Mucho se ha debatido en la historia doctrinal contemporánea la relación entre el delito fiscal y el blanqueo de capitales. Como esgrime De La Mata Barranco (2016: p. 8), a partir de la inclusión expresa que de la cuota fiscal defraudada hace la Ley 10/2010 (art. 1.2), no hay cabida a la interpretación; este efecto se considera como un bien con procedencia ilícita en relación con el delito de blanqueo de capitales[37]. Cuando un sujeto defrauda al Fisco, genera un ahorro de gastos que conlleva el aumento injustificado de su patrimonio. Así, la cuantía defraudada, que ahora obra en el haber del sujeto activo, conformaría el bien derivado del delito, susceptible de blanqueamiento (Blanco Cordero, 2011: pp. 22 y 23[38]). Ahora bien, tanto el delito fiscal como el blanqueo implican, directa o indirectamente, modelos de ocultamiento. Para no incurrir en una doble incriminación, impropia de un Derecho penal democrático, la procedibilidad del delito del 301 CP depende de que "continuaran realizando actos de ocultamiento —ahora sí— posteriores al delito tributario, que pudieran ser calificados como actos de blanqueo de capitales" (Castro Moreno, 2017: 148).

Las criptomonedas pueden dar lugar a diversos hechos imponibles, de acuerdo con la regulación de cada país: por su adquisición y venta, al ser un instrumento útil como medio de pago y de inversión; por su tenencia, que acrecienta la masa patrimonial del titular; por las ganancias y pérdidas de capital que generan sus variaciones de valor; por los servicios de intermediación realizados por algunos prestadores de servicios de criptoactivos; por la minería, como forma de actividad económica; por sus transmisiones lucrativas o gratuitas; etc. (Domínguez Martínez, 2023: pp. 4 y 5). Estos son conceptos que pueden ser gravados en diversas categorías de impuestos. De ahí

[37] Aunque, a diferencia de otros delitos como el de tráfico de drogas, en el delito fiscal no se produce un comportamiento prohibido que da origen a los bienes en sí, sino que devienen de negocios jurídicos lícitos, como las ganancias derivadas del trabajo o las ganancias patrimoniales resultantes de una venta (De la Cuerda Martín, 2017: p. 125).

[38] El estudio analizado, de gran relevancia en la temática abordada, explora con detenimiento el nexo causal que explicaría el origen de los bienes en este contexto. Concluye que el dinero defraudado no estaría en el patrimonio del autor del delito si no hubiese realizado la conducta activa. Esto no significa que sea sencillo de resolver en un proceso penal, pues es reconocida por el TS la dificultad de concretar e individualizar los beneficios de la defraudación en el patrimonio del contribuyente. Y brinda dos posibilidades: "que la acción típica del delito de blanqueo de capitales recaiga sobre una parte del patrimonio del defraudador que obligatoriamente incluya todo o parte de la cuota tributaria" o "que se consiga identificar la cuantía constitutiva de la base liquidable sobre la cual no se han pagado impuestos". STS 974/2012, de 5 diciembre, FJ 37.

que la normativa fiscal haya comenzado a darle prioridad al ámbito cripto en los últimos años. La Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal concretó ciertas y específicas obligaciones para determinados contribuyentes, en lo que respecta a la tenencia y negociación de criptoactivos; sobre todo en materia de suministro de información de los saldos de los titulares de monedas virtuales, tanto a nivel nacional como en el extranjero[39]. Estas medidas han sido introducidas por el Real Decreto 249/2023. Así, en España ya se ha añadido un apartado específico para la tributación de "monedas virtuales" en la Declaración de la Renta.

Controlar los delitos fiscales implica un seguimiento detallado de las transacciones financieras y las obligaciones tributarias de los contribuyentes. Las medidas de cumplimiento fiscal, como las mencionadas, exigen la transparencia en la tenencia y las operaciones con criptoactivos. Esto dificulta que los fondos obtenidos mediante fraude fiscal sean blanqueados o, si lo hacen, que se pueda sostener la elusión de la justicia. La Organización para la Cooperación y el Desarrollo Económico (OCDE, 2021: p. 55) indica que los reportes de transacciones sospechosas —lo cual es de obligado cumplimiento para las instituciones financieras y otros profesionales— pueden proporcionar una mayor inteligencia y conocimiento a las autoridades gubernamentales. Más aún, considera el Organismo que la inclusión de los delitos fiscales dentro del basto catálogo de delitos previos del blanqueo de capitales, amplía los canales de cooperación internacional y refuerza el "intercambio directo de información y la asistencia legal mutua, tanto entre autoridades investigadoras y de enjuiciamiento fiscal como entre autoridades fiscales y no fiscales". Además, las normativas fiscales establecen un marco disuasorio, debido a que las sanciones y medidas preventivas contra los delitos fiscales también actúan como un freno para los potenciales blanqueadores. Un sistema fiscal más rígido hace menos atractivas las actividades delictivas. Es decir, al controlar los delitos fiscales a través de medidas de transparencia, trazabilidad y cumplimiento normativo, se cierra una de las puertas principales que los criminales utilizan para iniciar el proceso de blanqueo de capitales. Y en este sentido, cobran especial relevancia los asesores fiscales, cuyo buen hacer contribuye a la prevención de la lacra que es el blanqueo de capitales (Camacho Belmonte, 2017: pp. 304 y ss.; Sánchez Robert, 2023: pp. 561 y 562).

3. *La corrupción pública*

La corrupción pública o política engloba múltiples actuaciones indebidas por parte de funcionarios y autoridades públicas, como la prevaricación, el

[39] Véase la Exposición de Motivos de la norma.

cohecho, el tráfico de influencias o la malversación, entre otros. Todos ellos son delitos contra la Administración Pública y conforman comportamientos que socavan la legitimidad de las instituciones públicas (Chanjan Documet, et al., 2018: p. 12), la confianza en ellas y la capacidad de los ciudadanos de recibir un trato justo cuando se relacionan con entidades gubernamentales (Albanese & Artello, 2018: p. 30) y afectar el disfrute de los DDFF de las personas (Peters, 2018: p. 30). La corrupción no es un fenómeno nuevo, pero sí uno que ha recibido cada vez más atención de los reguladores y las distintas instancias sociales en los últimos años. Con la globalización ha comenzado a percibirse, además, como un problema de la comunidad internacional y no como un asunto de interés meramente interno de cada país (De la Cuesta Arzamendi & Blanco Cordero, 2017: pp. 266 y 267). La corrupción es el resultado de un conglomerado de factores que anidan en el sistema socioeconómico (Monteverde Valero, 2021: p. 131), tales como la cultura, el conflicto social, los incentivos ofrecidos y el grado de desarrollo (Labaqui, 2003: p. 163)[40]. Pero hay que evitar a toda costa que la corrupción se convierta en un fenómeno sistémico, pues es muy difícil de controlar, abordar y superar (Myint, 2000. P. 41).

La corrupción publica está estrecha e intrínsecamente vinculada con el blanqueo de capitales (Jiménez García, 2016: pp. 225-227). Así lo clarifica el GAFI, quien insiste en que se trata de una serie de delitos cuyo beneficio y/o ganancias normalmente son objeto de blanqueo de capitales (GAFI, 2010: p. 2[41]). Por eso, los instrumentos de lucha contra éste también son altamente útiles para prevenir contra la corrupción (Gomes Pereira & Fontana, 2019: p. 11). Dependiendo de la naturaleza del acto corrupto, dicho blanqueo se presentará de distintas formas. El mismo Organismo internacional especializado

[40] A estas causas se podrían sumar las propuestas en el estudio de Miranzo Díaz (2018, pp. 6 y ss.): impunidad, actividades individualistas, envidia, imitación o aprendizaje, debilidad regulatoria, baja profesionalización del sector público, falta de independencia de los gestores y agentes de control, monopolio en la toma de decisiones, opacidad entre los canales de comunicación públicos y privados y otros.

[41] La Resolución aprobada por la Asamblea General el 2 de junio de 2021 S-32/1 expresa lo que procede: "Nos esforzaremos por poner fin a la impunidad de la corrupción y por asegurar que la delincuencia no sea lucrativa, previniendo, detectando y disuadiendo de manera más eficaz la transferencia, la conversión y la ocultación de bienes derivados de la comisión de delitos de corrupción, intensificando los esfuerzos nacionales por penalizar adecuadamente los delitos de corrupción y enjuiciando a las personas involucradas en actos de corrupción y en el blanqueo de dinero, adoptando medidas nacionales para investigar, localizar, embargar preventivamente, incautar, decomisar y restituir dichos bienes, conforme a lo definido en la Convención, y reforzando la cooperación internacional en la recuperación de activos. Reconocemos que una asociación sólida y de confianza entre los Estados requirentes y los requeridos, en que ambos adopten medidas proactivas, es clave para el éxito de la recuperación y restitución de activos" (apdo. 43).

en el tema refiere varias, entre las cuales se destaca la colaboración de "guardianes" que pueden crear estructuras legales para lavar activos; el uso de jurisdicciones extranjeras u *offshore*; las transacciones individuales por parte de asociados cercanos, amigos y/o familiares en representación del blanqueador; o el uso de efectivo por su naturaleza anónima (GAFI, 2011: pp. 19-24).

Las modalidades comentadas son perfectamente parangonables con las criptomonedas. El concepto de "guardianes" abarcaría a los prestadores de servicios de criptomonedas, que cumplen obligaciones en materia de antiblanqueo de bienes. En segundo lugar, como ya ha sido expuesto, las criptomonedas permiten la transferencia rápida y fácil de grandes sumas de dinero a través de fronteras, sin necesidad de pasar por el sistema bancario tradicional, por lo que las jurisdicciones *offshore* son altamente frecuentes en los movimientos cripto. En tercer lugar, la universalidad de las criptomonedas permite que cualquiera pueda obtener unidades y diversificarlas, aunque sea en nombre de otro, sin que sea preceptiva una representación formal. Y finalmente, aunque son rastreables, las criptomonedas ofrecen un grado importante de privacidad, lo que facilita la integración de fondos ilícitos —como los provenientes de la corrupción pública— en la economía formal, tal como el dinero en efectivo. La inmediatez y carácter transnacional de las criptomonedas, a su vez, permite que pueda sobornarse a un funcionario de cualquier país (Ibrahimi & Arifi, 2022: p. 99) o que esté pueda desviar fondos públicos a jurisdicciones con menores controles en materia cripto.

Un estudio de regresión por países determinó que los países con un control de la corrupción más débil y más controles de capital tienden a una mayor adopción de criptomonedas, sugiriendo que tales activos pueden ser útiles para transferir ganancias de la corrupción y eludir los controles mencionados (Alnasaa, et al., 2022: p. 9). Elsayed (2023: p. 7; Hrytsai, 2023: pp. 86 y 87) considera que dicho trabajo, no obstante, no busca una relación causal en el fenómeno. Por eso, el autor propone algunas posibles razones: a. Los países con altos niveles de corrupción suelen contar con instituciones político-financieras más débiles, lo que puede significar una escasa confianza en el sistema bancario formal; b. Las criptomonedas reducen restricciones sobre el comportamiento corrupto, incluyendo los costos de transacción y el menor riesgo de ser descubierto por la privacidad que propugnan. Cabe destacar que las organizaciones criminales, que se valen de las criptomonedas para perpetrar sus fechorías, también incurren en la corrupción de empleados públicos y autoridades políticas para conseguir sus objetivos y eludir la acción de la justicia (Saldaña Taboada, 2017: p. 11), lo que provoca una retroalimentación criminal.

Un caso que representa y expone lo contenido en este subapartado es el de un exalcalde de una municipalidad de Chile. La Fiscalía del país le acusó de malversación de fondos públicos, cohecho y lavado de activos. De acuerdo

con la investigación realizada, se habría desviado más de un millón de dólares estadounidenses desde las arcas municipales para usos privados. Este desfalco habría supuesto graves recortes a los beneficios entregados a la entidad local y con ello, perjuicios a los vecinos (Oportot Campillay, 2024). Junto al imputado, se investigan a otras 9 personas —algunas de ellas también ostentaban cargos funcionariales— que conformarían una red criminal que juntaba a amigos y familiares para la sustracción de fondos públicos (Palazzo, 2024). Según el informe del Fiscal (Fiscalía de Chile, 2024), tal organización se valió de testaferros o supuestos proveedores que recibirían los fondos públicos para luego remitirlos al exalcalde. A partir de allí, los investigados emprendieron acciones dirigidas a blanquear las ganancias obtenidas, entre otras cosas, adquiriendo criptomonedas por un valor de 4 millones de pesos. Pero fue posible reconducir la investigación considerando las cuentas corrientes y la trazabilidad de los fondos. Fruto del trabajo de las autoridades, se retiró la militancia de aquel, se admitió —y ratificó después de ser apelada— su prisión preventiva y otras medidas cautelares para los acusados. En el Informe Final de la Contraloría Regional de Valparaíso[42] se constatan fallos sistémicos de transparencia y control en la Municipalidad, que seguramente fomentaron la sensación de impunidad, un claro factor criminógeno en este tipo de delitos. Sin lugar a duda, el fortalecimiento de controles internos es fundamental para prevenir la corrupción y el blanqueo de capitales que le suele acompañar, implementando medidas de transparencia rigurosas, auditorías periódicas y externas y la implementación de tecnología de trazabilidad financiera[43].

Ahondando en la última cuestión, no pocos países han implementado soluciones basadas en *blockchain*, e incluso normativas específicas para explotar su potencial, para mitigar la corrupción (Figueroa Castillo, et al., 2021: pp. 103 y ss.). De hecho, su transparencia e inmutabilidad le hacen ser

[42] Puede consultarse en el siguiente enlace: https://interferencia.cl/sites/default/files/cgr-algarrobo-sello-agua.pdf. Consultado por última vez el día 31 de julio de 2026. Algunos de esos fallos son: la ausencia de manuales que describan los procedimientos administrativos relacionados con la tesorería municipal, la no formalización por acto administrativo de algunos cargos, la carencia de protección de nóminas de pago a proveedores para evitar adulteraciones, la escasa determinación de conciliaciones bancarias, etc.

[43] De ahí que se esté otorgando especial interés a las personas expuestas políticamente. SEPBLAC (2008, p. 7) lo explica de la siguiente forma: "Se trata de una clasificación específica en tanto que lo característico no es el tipo de operación que se realiza, ni siquiera el sector de actividad o de negocio en el que se integran los fondos, sino la condición política que tiene el propietario de estos. Cada vez con más fuerza surge la necesidad de reforzar los controles de las operaciones en las que se implican estas personas, sus familiares directos y las personas relacionadas, al ser especialmente sensibles al blanqueo de capitales procedentes de delitos relacionados con la corrupción".

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

una tecnología casi imposible de adulterar (Carpio, 2018: p. 6). No obstante, quienes tendrían que implementar estos modelos tecnológicos con fines de anticorrupción pueden mostrarse reacios a crear un registro inmutable y transparente de todas sus actividades (Aggarwal & Floridi, 2019: p. 2). Además, el Foro Económico Mundial (FMI, 2021) refiere que, al ser una solución innovadora, los Gobiernos deben verificar el momento adecuado para adoptarla, especialmente la educación de los ciudadanos.

4. *La corrupción privada*

El académico Morillas Cueva (2023: pp. 40 y 41) propone el siguiente concepto de corrupción, tras analizar la complejidad de construir una definición para una manifestación criminal tan polifacética: "conducta de persona dotada de poder de decisión que, con abuso de él, incurriere en actividad desleal a sus funciones y cargo en el ámbito público o en el sector privado de relaciones comerciales para conseguir por petición directa propia o por ofrecimiento de otro, o con su actuación distrajere bienes públicos o privados, con la finalidad de obtener para sí mismo o para un tercero una ventaja o beneficio económico o de otra índole". La globalización de la economía y los mercados ha influido decisivamente también en la expansión de la corrupción en el ámbito privado (Sánchez Bernal, 2010: p. 220; Otero González, 2012: p. 176). Los escándalos que han tenido lugar en los mercados financieros y compañías de renombre han generado, en palabras de Carbajo Gascón (2012: p. 186): "una ola de desconfianza y malestar de los ciudadanos en las grandes empresas, en las instancias del poder político de control de los mercados e incluso en el mismo sistema económico de referencia mundial […] a la vista de las graves consecuencias que tales escándalos han traído consigo para el funcionamiento eficiente del mercado y para la consecuente satisfacción de los intereses públicos o generales en el funcionamiento correcto del sistema de economía de mercado, así como, indirectamente, para los intereses particulares de los ciudadanos en sus condiciones respectivas o sucesivas de trabajadores, inversores, depositantes o impositores, asegurados o consumidores".

La intervención del Derecho penal en supuestos corruptos dentro de la esfera particular se ha justificado para la protección de la competencia leal, en aras de evitar que las relaciones comerciales estén definidas por factores ajenos o sean monopolizada por actores poco escrupulosos y sin ética (Castelló Nicás, 2022: p. 51[44]). Se tipifica como delito en el art. 286 bis, tanto su vertiente pasiva, como

[44] En un abordaje bastante crítico, Bolea Bardón (2016: p. 110): concluye que "lo que se intenta proteger a través de este delito es la afectación de la capacidad competitiva de la empresa *ad extra* y *ad intra*, esto es: por un lado, el interés de los terceros competidores

la activa. En ambos casos, un elemento típico es el beneficio o ventaja "de cualquier naturaleza" que se da a los sujetos adscritos a la empresa o sociedad mercantil, lo que cubre sin lugar a duda a las criptomonedas. Nuevamente, puede coexistir simultáneamente con otras figuras delictivas, como advierte Sánchez Robert (2021: p. 651), como el blanqueo de capitales, los delitos fiscales y otras formas de corrupción. La autora razona el porqué de tal conclusión basándose en los elementos comunes que aprecia en estos delitos: "el movimiento de grandes sumas de dinero, el enriquecimiento desproporcionado de algunas personas, la utilización de redes de sociedades interpuestas, y la utilización de testaferros, sociedades pantalla y paraísos fiscales".

Aunque no hay estudios previos —al menos a los que la escritora pudiera tener acceso— que relacionen los criptoactivos con la corrupción privada, los riesgos perceptibles en el caso anterior lo son también en este caso. Los activos virtuales pueden ofrecerse como beneficio a un directivo, empleado o representante de una empresa, a cambio de obtener un trato preferencial, acceso a información privilegiada o la adjudicación de un contrato comercial. Dentro del mismo ámbito empresarial, aquellos fondos pueden transferirse a sociedades pantalla o testaferros, que luego los canalizan al destinatario final. De esta forma, se puede ocultar la ventaja obtenida con la comisión del delito y, por tanto, dar lugar a su blanqueo.

IV. PROBLEMÁTICAS ESPECÍFICAS ASOCIADAS A LA PERSECUCIÓN DEL BLANQUEO DE CAPITALES CUANDO INTERVIENEN CRIPTOACTIVOS

1. *Los "muleros"*

Tan amplísimo es el delito básico de blanqueo de capitales como su modalidad imprudente: "Si los hechos —tipificados en los apartados previos— se realizasen por imprudencia grave, la pena será de prisión de seis meses a dos años y multa del tanto al triplo" (art. 301.3 CP). La definición de la conducta se resume a "los hechos", siendo que previamente se exige el conocimiento del origen ilícito de los bienes por parte del sujeto activo y la intención de ocultar los bienes o favorecer a los delincuentes. Estos elementos típicos han hecho que no sea indubitable el encuadre de la forma imprudente del delito (Fabián Caparrós, 2010: pp. 67 y ss.[45]). Pero no ha sido

en no quedar desplazados por ofertas claramente peores que, sin embargo, son preferidas por venir acompañadas de incentivos, beneficios o ventajas; y, por otro, el interés de la propia empresa en que el encargado adquiera bienes o servicios que constituyan la mejor oferta en el mercado".

[45] Explica que ha sido necesaria una interpretación correctora de la norma, que preserve su vigencia respetando la voluntad del Legislador. También indica que la amplitud de la

pacífica su aceptación doctrinal[46]. La jurisprudencia ha intentado aclarar algunas de las cuestiones más debatidas. Por ejemplo, la STS 506/2015 (FJ 5)[47] indica: a. que actúa con imprudencia "quien ignora el origen ilícito de los bienes por haber incumplido el deber objetivo de cuidado que impone el art 301 3º"; b. que la imprudencia recae en el conocimiento de la procedencia delictiva de los bienes y no sobre la conducta en sí misma; c. que el sujeto en cuestión estaba "en condiciones de sospechar fácilmente la ilícita procedencia y de evitar la conducta blanqueadora sólo con haber observado la más elemental cautela". Los adjetivos fácilmente y elemental exigen una observancia mínima por parte del agente, por lo que basta con la conciencia de que se trata de una operación anormal y la inferencia razonable de que los fondos proceden de cualquier actividad delictiva (Caba Tena, 2022).

fórmula del delito, que incluye cualquier otro acto no incluido dentro de los verbos rectores expresos, puede sortear la limitación de este tipo intencional para aplicar la imprudencia.

[46] Por ejemplo, Fernández Cruz (2005: p. 162) aprecia que la tipificación del blanqueo imprudente no colisiona con las exigencias del principio de intervención mínima, en relación con la teoría del bien jurídico; no es coherente con el mandato de certeza que debe regir a la normativa penal, al no quedar clara cuáles omisiones de obligaciones de diligencia dan lugar a la activación de esta forma delictual; se erige como un tipo de "sospecha"; entre otras cuestiones. Aránguez Sánchez (2020: p. 278) por su parte, considera que la modalidad estudiada colide con la irrelevancia penal de la imprudencia en los delitos socioeconómicos y que externamente las transacciones de blanqueo no se distinguen de los movimientos de dinero lícito. Sin embargo, Souto (2022, p. 195) entiende que la previsión legal del blanqueo imprudente no conculca ningún principio propio del Derecho penal ni exigencia constitucional alguna. Concluye que no se produce una vulneración del principio de taxatividad, pues es una formula flexible habitual en los tipos imprudentes; ni tampoco del principio de intervención mínima, considerando que el objetivo estatal del delito de blanqueo es comprometer a toda persona, no solo a determinados profesionales, a proteger un bien jurídico supraindividual.

[47] En relación con ella, la STS 412/2014, 20 de Mayo de 2014, FJ 2 dice: "La imprudencia se exige que sea grave, es decir, temeraria. Así en el tipo subjetivo se sustituye el elemento intelectivo del conocimiento, por el subjetivo de la imprudencia grave, imprudencia, que por ello recae precisamente sobre aquel elemento intelectivo. En este tipo no es exigible que el sujeto sepa la procedencia de los bienes, sino que por las circunstancias del caso esté en condiciones de conocerlas sólo con observar las cautelas propias de su actividad y, sin embargo, haya actuado al margen de tales cautelas o inobservando los deberes de cuidado que le eran exigibles y los que, incluso, en ciertas formas de actuación, le imponían normativamente averiguar la procedencia de los bienes o abstenerse de operar sobre ellos, cuando su procedencia no estuviere claramente establecida. Es claro que la imprudencia recae, no sobre la forma en que se ejecuta el hecho, sino sobre el conocimiento de la naturaleza delictiva de los bienes receptados, de tal modo que debiendo y pudiendo conocer la procedencia delictiva de los bienes, actúe sobre ellos, adoptando una conducta de las que describe el tipo y causando así objetivamente la ocultación de la procedencia de tales bienes (su blanqueo) con un beneficio auxiliador para los autores del delito de que aquéllos procedan".

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

La modalidad imprudente de blanqueo ha sido la figura normalmente aplicada a las "mulas de dinero" o los "muleros". Se trata de sujetos que transfieren activos a una persona, habiéndolos recibido de otra, a cambio de una comisión. En el contexto concreto del blanqueo de capitales y la financiación del terrorismo, las mulas se convierten en una vía de asistencia financiera con la que personas que, en principio, no tenían motivaciones criminales, acaben siendo responsables penalmente por crímenes muy graves (Pickles, 2021: p. 239[48]). Además, frecuentemente los delincuentes no se valen de una única "mula de dinero"; dependiendo del delito pueden conformar una red de ellas. La evolución continua del espacio digital amplifica estos riesgos, lo que exige una mayor vigilancia y proactividad para prevenir el fenómeno (KPMG, 2024: p. 2). Incluso, es factible que se pirateen los perfiles y las cuentas de las potenciales "mulas" para que, sin que ellas medien de forma consciente, se remitan los fondos ilegales en su nombre y se ofusque su trazabilidad (Abdul Rani, et al., 2022: p. 154[49]). Por tanto, el reto es bastante amplio: mitigar los riesgos asociados con la expansión del espacio digital y la sofisticación de las técnicas de los criminales.

El SEPBLAC (2024 a: p. 17) inquiere a los sujetos obligados estar al tanto de las posibles cuentas mula, advirtiendo la concurrencia de las siguientes características: inmediatez entre la entrada y la salida de los fondos recibidos, nivelación del saldo, transferencias como principal vía de entrada de fondos, inutilización de la cuenta para actividades financieras habituales dentro de su país, diferencias entre el nombre señalado como beneficiario de las transferencias abonadas y el nombre del titular de la cuenta, incongruencia

[48] No obstante, Del Mónaco (2020: p. 10); basándose en estudios de EUROPOL, subraya que las personas más expuestas a ofertas para ser "mulas" son inmigrantes recién llegados al país de destino, desempleados, estudiantes y personas con dificultades económicas. Según el rango de edad, el objetivo suele ser menores de 35 años, aunque los criminales han comenzado a reclutar generaciones aún más jóvenes.

[49] En estos casos, obviamente las ficticias "mulas" no merecerían ninguna responsabilidad penal. Los delincuentes darían lugar a un concurso medial de delitos, en relación con el blanqueo de capitales y el intrusismo informático, siendo este último el vehículo facilitador para perpetrar aquel. También es común que la presencia de las "mulas" en el ámbito cripto para blanquear dinero resulte del ofrecimiento de un supuesto trabajo; un tipo de estafa muy conocida. Souto (2022: p. 19) remarca el aumento que estas ofertas tuvieron durante la pandemia por COVID-19. Es visible que la selección de potenciales mulas no es una casualidad, sino que se basa principalmente en aprovechar la vulnerabilidad económica de las personas para que sea más difícil que se cuestionen la propuesta y simplemente acepten. Por su parte, el GAFI (2020: p. 11) advierte que los delincuentes pueden aprovecharse de personas mayores u otras que no comprenden la tecnología de los activos virtuales para que se conviertan en "mulas". De hecho, en algunos casos, estos solicitaban la instalación de un controlador remoto de dispositivos, para que pudieran ayudar a las iniciales víctimas a transferir los recursos de forma correcta.

entre el concepto de pago señalado por el ordenante y el conocimiento de las entidades sobre la actividad del titular de la cuenta, operaciones internacionales no justificadas, indicios de que el titular no actúa por cuenta propia, falta de aportación de información sobre la operativa de la cuenta y cuentas de contratación reciente o inactivas que se reactivan sin razón aparente. Tal Unidad Financiera española ha modificado recientemente el formato con el que los sujetos obligados le comunican las operaciones que presenten indicios de blanqueo de capitales, pudiendo ahora enviar tantas comunicaciones distintas como tramas sea capaz de detectar y analizar e incluso, agrupar en una misma comunicación datos sobre varias cuentas mula (SEPBLAC, 2024 b: p. 1). Esto es una evidencia clara del aumento y la sofisticación de las redes de mulas de dinero en actividades de lavado de capitales y financiamiento ilícito. La inclusión de características específicas y el énfasis en nuevas medidas de reporte reflejan cómo estas redes han evolucionado y ampliado su alcance, aprovechándose de herramientas tecnológicas y lagunas en los sistemas de control. Y la respuesta del SEPBLAC indica un esfuerzo por adaptarse a este fenómeno, subrayando la urgencia de implementar medidas más efectivas y colaborativas entre entidades financieras y autoridades para contrarrestar este problema.

No es que la figura de las "mulas" ha sido desplazada por los criptoactivos, sino que su trabajo es más accesible con la intervención de éstos. Los "muleros" ya no necesitan operar con sus cuentas bancarias, pudiendo los bancos ver las transacciones en tiempo real y siendo capaces de interrumpirlas y denunciarlas a las entidades correspondientes. Las criptomonedas son pseudónimas desde su creación, se necesitan pocos segundos para crear una billetera criptográfica y es gratuita, se pueden realizar miles de transferencias a bajo costo y ejecutarlas mediante una secuencia informática de comandos y se hacen efectivas en poco tiempo[50]. Por tanto, las "mulas" de criptomonedas pueden operar preservando en mayor grado su identidad; generando múltiples *wallets* para dispersar más el gasto; invertir menos dinero en comisiones y mover activos ilícitos en menos tiempo a múltiples jurisdicciones, lo que permite que más rápido se deshagan de su tenencia.

Es difícil medir el fenómeno de las "mulas" de activos a través de billeteras cripto y perseguir cada supuesto, pero puede limitarse con el establecimiento de agencias de control, que son los sujetos obligados. En el estudio del *Financial Intelligence Centre* de Sudáfrica (2024: p. 7) se informa que 137 reportes relacionados con "mulas de dinero" han sido emitidos por los

[50] Estas son las características específicas que identifica EUROPOL en el blanqueo de activos mediante criptomonedas. Puede consultarse en el siguiente enlace: https://syntheticdrugs.unodc.org/syntheticdrugs/es/cybercrime/launderingproceeds/moneylaundering.html.Consultado por última vez el día 31 de julio de 2026.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

bancos de la región desde 2016 a 2023 y 9 reportes por parte de los prestadores de servicios de criptomonedas en la misma franja temporal. Aunque parezca una diferencia importante, ambos están de primeros en la tabla y hay que sopesar dos cosas. Primero, las transacciones bancarias son mucho más trazables y menos ofuscadas, lo que justifica que estas entidades tengan mayor grado de control e intervención y se generen más reportes. Segundo, las "mulas" con criptomonedas no han sustituido las primeras, sino que han sumado una oportunidad más para los delincuentes (AUSTRAC, 2024: p. 15). Por eso los esfuerzos regulatorios se han intensificado en torno a los prestadores de servicios de criptoactivos, en sentido amplio, reforzando su asimilación como sujetos obligados. Una buena guía para identificar tempranamente posibles "mulas" y reportarlas a la Unidad Financiera son los indicios del GAFI (2020: p. 10):

– El remitente no parece estar familiarizado con los activos virtuales o soluciones en línea de custodia de los mismos. Puede indicar que ha sido reclutado por blanqueadores de activos o que han sido víctimas de estafas previas para convertirlas en "mulas".
– El remitente tiene una edad mayor que el promedio de usuarios de la plataforma, ha abierto una cuenta y realiza un gran número de transacciones. Es un indicio de que se trata de una "explotación financiera de ancianos".
– El remitente es una persona financieramente vulnerable.
– El cliente compra cuantiosas cantidades de activos virtuales no justificado por su patrimonio disponible ni coherente con su perfil financiero histórico.

Finalmente, cabe mencionar que ya se han producido estudios que proponen el uso de herramientas predictivas para detectar posibles "mulas" en *exchanges* de criptomonedas. Por ejemplo, Kerzic (2022: pp. 14 y ss. y 52) probó el empleo de modelos de análisis predictivo con algoritmos de aprendizaje supervisado con la creación de modelos de regresión logística, árbol de decisión y métodos de ensamble[51]. Sin embargo, el investigador reconoce que, aunque el sistema es capaz de predecir comportamientos fraudulentos, no anticipa todos los casos positivos y en otros casos, ofrece falsos positivos. En torno a estos segundos casos, reflexiona que deberían ser investigados, lo que implicaría utilizar muchos recursos sin éxito garantizado. Ribeiro Pereira (2021: pp. 49 y ss.), en contraste, propone el desarrollo de clasificadores que

[51] Los métodos de ensamble son técnicas que permiten mejorar el rendimiento de la predicción de un modelo de aprendizaje profundo, como modelos bayesianos, *bagging*, *random forest*, *boosting, stacking,* etc. Estas técnicas aprovechan la diversidad de los modelos individuales para reducir errores como el sesgo, la varianza, o el ruido.

discriminen entre transacciones lícitas y que persiguen el blanqueo a partir de redes generativas antagónicas.

2. *Las* Initial Coin Offerings *(ICOs)*

Las ICOs son proyectos de captación de capital para propuestas y/o emprendimientos en etapa inicial. En el caso de los criptoactivos, las plataformas solicitan financiación externa emitiendo *tokens* o unidades de criptomonedas. Tienen beneficios frente a otras formas de recaudación, como los bajos costos del proceso, la ausencia de terceros voluntarios, la proyección sobre proyectos basados en tecnología Blockchain y los umbrales de inversión más bajos (Campino, et al. 2022: p. 3). Se puede llevar a cabo con el ofrecimiento de *tokens* de utilidad, de seguridad o directamente con criptomonedas. Si lo que se pretende es preservar un alto grado de privacidad o un potencial anonimato, los primeros han sido los menos regulados, por lo que puede ser la opción preferente en estos casos (Momtaz, 2020: p. 7).

En el anuncio de presentación de cualquier ICO los promotores suelen brindar un resumen ejecutivo de la idea, pero sus características detalladas se ofrecen en un *white paper*[52] particular. Estos documentos tienen un contenido muy diverso, muchas veces con poca información financiera para los consumidores (Vieira Dos Santos, 2020: pp. 41 y 42). Además, pocas veces contienen especificaciones sobre la jurisdicción donde operará la iniciativa de que se trate (Moxotó, et al., 2021: p. 4182). En realidad, su precisión es muy importante pues permite medir el alcance de un proyecto cripto y su tecnología subyacente, según lo cual los interesados decidirán si invierten o se involucran en él. Como es un vehículo para la generación de confianza, puede manipularse para lograr ese objetivo sin realmente respetar las garantías mínimas para un proyecto cripto fidedigno. Sus autores pueden: suprimir o ignorar deliberadamente datos importantes, ofrecer promesas exageradas sin sustento o plasmar ambigüedades legales del proyecto de forma intencionada (Policía Metropolitana de Reino Unido, 2024: p. 9). En vista de lo anterior, las autoridades podrían buscar señales de posibles riesgos de blanqueo de capitales en los proyectos cripto emergentes, aunque se enfrentan con el hándicap de que son documentos sin un formato obligatorio que les permita hacer comparaciones analíticas.

El Reglamento europeo sobre los criptoactivos (MiCA) ha establecido unos mínimos en relación con el contenido de los libros blancos y trámites

[52] Un libro blanco es un documento técnico o informativo contenedor de información detallada sobre un tema, proporcionando datos, análisis y propuestas fundamentadas. En el caso de las criptomonedas, el *white paper* permite exponer con detalle la tecnología, los objetivos, las características y el funcionamiento del proyecto.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

burocráticos previos a su publicación; salvo en algunos supuestos dependiendo del criptoactivos de que se trate[53]. La potencial exclusión que la norma hace de las criptomonedas con emisión privada hace que estas exigencias no sean plausibles en muchos casos, pero indica claramente un interés de los reguladores europeos por prevenir delitos desde fases iniciales, como la elaboración del libro blanco. Kryptomat (s/f) expone algunas "banderas rojas" en los *white papers*, es decir, señales de advertencia de posibles intenciones deshonrosas y deshonestas: ausencia de detalles técnicos básicos o vaguedad en la exposición de los que contiene, promesas desorbitadas sin un plan realista, plagios de otros proyectos[54], afirmaciones que no pueden comprobarse, falta de información sobre el equipo de la iniciativa, priorizar aspectos comerciales y no criterios puramente técnicos comprensibles y errores ortográficos y gramaticales visibles.

Usualmente el estudio sobre el potencial delictivo de las ICOs se centra en las estafas y la protección del consumidor. Sin embargo, también conciernen riesgos para blanquear activos. El blanqueo puede consumarse tanto proponiendo proyectos de este tipo falsos, presentando un libro blanco aparentemente legítimo para ganar la confianza de inversores y mezclar sus fondos con los ilícitos previamente obtenidos; como comprando grandes cantidades de *tokens* o unidades de criptomonedas ofrecidas en una ICO para luego venderla. La ESMA (2017: p. 1) advirtió que tales iniciativas suelen ser espacios no regulados —aunque, como se ha visto, cada vez más Estados comienzan a dar pasos hacia normativas aplicadas a ellas—; cuestión que favorece su utilización criminal (Essaghoolian, 2019: p. 342)[55]. Además, la vocación transnacional de las ICOs hace que, incluso cuando se emitan regulaciones específicas, se pueda participar o lanzar dichos proyectos en otras jurisdicciones del mundo. Por eso, la mejor opción en estos casos es proyectar las obligaciones de diligencia debida y de KYC a los operadores e intermediarios de las ICO (De Andrés, et al., 2022: p. 5), cuando no sea una propuesta privada e individual.

[53] Afirman Angurem et al. (2023: pp. 130 y 131) que la supervisión y autorización —en determinados casos— de los libros blancos de criptoactivos que deben hacer las entidades gubernamentales las convierte en supervisores "de los sujetos y la actividad regulada en MiCA".

[54] Esto es interesante, pues otros trabajos, como el de Camassa (2023: p. 140), sugieren que si un libro blanco presenta información nueva o adicional que no está disponible en otros documentos similares sería más esclarecedor. Sin embargo, un inversor o investigador de un caso concreto puede no tener los recursos necesarios para tomar una muestra suficientemente amplia de libros blancos como para medir sus coincidencias y disparidades.

[55] En Estados Unidos el Departamento de Justicia puede imponer sanciones penales contra los desarrolladores, administradores y terceros involucrados cuando los fondos de la ICO se destinan a objetivos distintos a los previstos o incluso, acordar la rescisión de los *tokens* cuando comprueban que ha habido mala fe.

3. *Las* self-custody wallets

La historia económica ha ido derivando a un segundo plano la autocustodia de los bienes, posicionando a los bancos como guardianes de ellos. En el caso de las criptomonedas, la posición protectora de tales entes se diluye de sobremanera, pero se erigen otros custodios, los prestadores de servicios con criptoactivos. Cuando los usuarios deciden confiar sus activos virtuales en estas plataformas sujetas a una comprehensible regulación, renuncian al control exclusivo de aquellos y minimizan los efectos descentralizados de la criptografía aplicada al ámbito económico (Erinle et al., 2025: p. 3[56]). Debido a eso, en la taxonomía propuesta por Jaroucheh y Ghaleb (2023: p. 2), los criptoactivos que están bajo la custodia de profesionales o instituciones dedicadas a ello, conforman un supuesto de custodia total, bajo la lupa de la normativa antiblanqueo. Sin embargo, en un orden distinto se ubica la autocustodia de los mentados activos, donde los propios usuarios mantienen y administran los que poseen. El último supuesto puede presentarse con almacenamiento en frío, billeteras de *hardware*[57] o almacenando las claves criptográficas en libretas o algún escrito físico. Es un serio desafío averiguar quién tiene acceso o controla las criptomonedas administradas por los propios usuarios sin ningún tipo de intermediación (Taylor et al., 2022: p. 15).

Los reguladores tienen delante de sí el reto de producir normativas equilibradas para la protección de los inversores y del sistema socioeconómico, sin derrumbar un mercado emergente, ágil, innovador y competitivo. Y también necesitan reducir las brechas existentes en áreas donde la regulación no es tan eficiente, como el de las billeteras autoalojadas. No se puede asumir

[56] Los proveedores de servicios de criptoactivos y, en este contexto principalmente los custodios, están obligados a cumplir con la diligencia debida, normativa de gobernanza, realizar auditorías, contar con coberturas de seguros e implementar medidas de seguridad cibernética —y física, en su caso—.

[57] Este tipo de billeteras, como la conocida *Trezor*, son máquinas diseñadas para almacenar claves privadas fuera de línea, con el objeto de proteger y asegurar los criptoactivos, principalmente. Para comprar estos dispositivos no es necesario suministrar datos, lo que impide identificar con facilidad a los propietarios de tales billeteras. En vista de ello, Lawrence (2022) indica lo siguiente: "Una vez que está en posesión de un malhechor, solo necesita evitar realizar transacciones con billeteras alojadas en bolsas de criptomonedas que realizan actividades KYC/AML para mantener un perfil bajo. Esto significa que pueden recibir fondos y enviar fondos a billeteras alojadas en ellas mismas (es decir, billeteras de hardware) en todo el mundo con un riesgo mínimo de monitoreo por parte de terceros. Algunos dispositivos también permiten a los usuarios comprar criptomonedas a través de una interfaz con bolsas de mayor riesgo que realizan distintos niveles de KYC/AML que se pueden eludir fácilmente. Estas bolsas también se pueden utilizar para convertir una criptomoneda en otra (es decir, bitcoin en Monero), lo que puede servir como contramedida contra el análisis forense de la cadena de bloques".

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

que todo aquel que opte por custodiar y administrar por sí mismo sus criptomonedas tiene intenciones ilícitas, pues muchos usuarios lo hacen simplemente con el fin de eliminar los riesgos que supone confiar sus bienes a un tercero (World Federation of Exchanges, 2024: p. 6), alineándose así con la naturaleza originaria de esta tecnología financiera. Hay que ser realistas: la custodia personal de criptomonedas no puede ser objeto de una regulación con proyección práctica viable. Esta actividad no requiere registro ni permisos de ninguna entidad centralizada, no está vinculada a una identidad directamente ni hay entidad o intermediario alguno responsable de los fondos. Sin embargo, como esas billeteras seguramente se interconectarán con otras que sí están negociadas y gestionadas con intermediarios que cumplen medidas de diligencia debida y la regla de viaje, se podrán obtener datos de partida por parte de tales entidades para emprender labores de investigación que no serán nada sencillas. Probablemente, el sector más regulable del fenómeno son las empresas o plataformas que ofrecen servicios o productos relativos a la *self-custody* de criptomonedas, como los promotores de billeteras de *hardware.*

Ilustrativo de lo advertido en el párrafo que precede es el caso de *Samourai Wallet*. Las autoridades de EEUU inculparon a los CEO de esta compañía e intervinieron el sitio web oficial por, entre otros delitos, blanqueo de capitales. Además, el FBI advirtió que operaban con funciones de servicios monetarios, pero no estaban registrados como tal. Por ello, se está planteando la necesidad de establecer licencias de transmisores de dinero para herramientas de autocustodia de criptoactivos en el futuro, según informa Cointelegraph Research (2024[58]). En el informe emitido por la Fiscalía de los Estados Unidos (2024) se explica el funcionamiento de *Samourai*, que ofrecía dos servicios:

a. *Ricochet*: "Es un tipo de transacción exclusivo de Samourai. Ricochet se defiende contra las listas negras de bitcoins agregando transacciones adicionales de señuelo entre el envío inicial y el destinatario final. Debería considerar usar Ricochet cuando envíe a casas de cambio de bitcoins y empresas que son conocidas por cerrar cuentas por razones poco sólidas"[59]. La función mencionada permite rebotar transacciones

[58] No obstante, no está claro cómo garantizar que todo aquel que vive en determinadas jurisdicciones —puesto que hay que considerar que la exigencia de determinadas licencias tiene una vocación estrictamente regional— va a someterse a tal exigencia en caso de querer utilizar criptomonedas sin custodia, en tanto puede conectarse desde servidores extranjeros o incluso ejecutar tal práctica en su intimidad.

[59] Así se presentaba el servicio en la documentación de *Samourai*, aunque ya el dominio se ha dado de baja y no está disponible para su consulta. Hay dos cuestiones destacables en la descripción del servicio: *Ricochet* estaba diseñado abiertamente para eludir

salientes con direcciones intermedias antes de que llegue a su destinatario (Floriane, B., 2019). Es, en consecuencia, una forma de reforzar tu privacidad al enmascarar el rastro de una transacción, aunque tiene un costo adicional por hacerlo[60].

b. *Whirlpool*: Un servicio de mezcla basado en modelos *CoinJoin*, donde un grupo de usuarios combina los fondos que quieren transferir en una sola transacción grande, lo que genera múltiples entradas y múltiples salidas con cantidades iguales o similares (Ghesmati et al., 2022: p. 29). Desde afuera, es casi imposible saber qué entrada corresponde a qué salida. Por tanto, la ofuscación de la identidad de las partes es absolutamente reforzada.

La investigación del caso[61] resultó en indicios claros de que las herramientas de autocustodia ofrecidas por *Samourai* perseguían la prestación de un servicio criminal para blanquear fondos. Para comprobar el conocimiento y la intención de los fundadores de la plataforma, los investigadores analizaron hilos de *Twitter* —ahora *X*— publicados desde sus perfiles oficiales, chats y mensajes privados, base de clientes inclusiva con delincuentes —lo cual incluso era promovido a nivel de *marketing*—, entre otras cuestiones. Lo cierto es que la complejidad de estos supuestos obliga a los operadores jurídicos y reguladores a seguir examinando la realidad práctica, en aras de mantener actualizada la regulación. La intervención de *Samourai* envió un mensaje claro sobre los riesgos criminales de la autocustodia de criptoactivos, desencadenando propuestas para hacer frente a estos casos. Un ejemplo de ello es la propuesta de crear identidades digitales rastreables reguladas a nivel federal para todas las billeteras y usuarios (Wagner, 2023). Es una alternativa ambiciosa que no tiene precedentes que avalen su potencial. Sin embargo, no soluciona ni remotamente el problema que significa el carácter transnacional del mundo cripto y la posibilidad de conectarse a servidores externos.

4. *El método* proof-of-burn

Un algoritmo de consenso alternativo y único en el mundo de las criptomonedas, aunque aún poco frecuente y escasamente estudiado, es el *proof-of-burn* o prueba de quemado. Este protocolo permite transferir activos

mecanismos de control y se presentaba como una especie de necesidad por limitaciones supuestamente injustificadas por parte de los sujetos obligados.

[60] Las tarifas de minería son más altas, porque ocupa más espacio en la cadena de bloques.

[61] Llevada a cabo por la Unidad de Fraudes Complejos y Delitos Cibernéticos y de la Unidad de Financiamiento Ilícito y Lavado de Dinero de la Fiscalía.

virtuales de una cadena de bloques a otra, "quemándolos" de la primera y creándolos nuevamente en la segunda. También se manifiesta en enviar los fondos a una dirección especial de la que nunca se puede retirar —en la práctica, es como si se suprimiesen del universo cripto—, a cambio de *tokens* (Rodinko et al, 2024) o recompensas similares a las que reciben los mineros[62]. Aunque no es una práctica conocida, esta arquitectura informática puede ser explotada para el blanqueo de capitales, cuando los delincuentes manejan criptomonedas que se puedan negociar en una cadena de bloques que funcione con este protocolo de consenso.

Quemar activos virtuales permite eliminar cualquier rastro directo de propiedad, lo que permite a los criminales tener una vía de escape, en caso de que estén siendo investigados o se sospeche de ellos. Por otra parte, estos sujetos podrían adquirir criptomonedas de origen ilícito, quemarlas a través del *proof-of-burn* y recibir estipendios u otros activos virtuales recién generados, que no tengan vínculo directo con los fondos originales, ya suprimidos del historial del gran libro de registros que es *blockchain*. La "quema" permanente de monedas dificulta la recuperación de activos quemados como evidencia para investigaciones financieras. Por eso, las plataformas que implementan el susodicho protocolo deben adherirse también a las políticas antiblanqueo si se configuran como sujetos obligados dentro de la categoría de prestadores de servicios de criptoactivos.

5. *Los* Non-Fungible Tokens *(NFT)*

Aunque el objeto material de este trabajo se centra en las criptomonedas dentro del gran universo cripto, es perentorio incluir un análisis sobre los NFTs en la cuestión relativa al blanqueo de capitales. Estos *tokens* son "activos criptográficos en una cadena de bloques con códigos de identificación únicos y metadatos que los distinguen entre sí" (Peres et al, 2022: p. 3). A diferencia de las criptomonedas, los NFTs representan algo único, por lo que no son fungibles[63] ni reemplazables, ni tampoco pueden fragmentarse en unidades más pequeñas (Blanco Escinosa, 2023: pp. 3 y 4). El valor de tales fichas se basa en

[62] De acuerdo con la descripción técnica ofrecida por Karantias et al. (2020: p. 3), el usuario A genera una dirección codificada como *BurnAddr*, donde envía sus criptomonedas y el usuario B recibe los datos de la transacción e invoca el código *BurnVerify*, para verificar que se destruyó de forma irrevocable la cantidad convenida por aquel. Además, apunta el estudio de Fu et al. (2021: p. 6) que el minero que quema la mayor cantidad de criptomonedas durante un período será líder en la generación de un nuevo bloque, es decir, tendrá preferencia prioritaria para validar.

[63] Algunos autores, como Proaño (2024: pp. 160 y 161, han intentado suavizar la no fungibilidad de los NFTs, al indicar que no hay barrera técnica o jurídica que impida que sean potenciales activos fungibles, pues lo relevante no es su *hash* sino su contenido. Sin

el interés del consumidor, su accesibilidad, el prestigio del autor, su historial de propiedad y la tangibilidad y exclusividad (EY, 2022: p. 4). Ahora bien, al igual que las criptomonedas su titularidad y datos de identificación se registran en la Blockchain, sobre todo en *Ethereum*, por su avanzada implementación de *smart contracts*[64]. Los NFTs y las criptomonedas interaccionan considerablemente, en la medida en que la mayoría de los sitios web que se dedican a la venta de los primeros, permiten pujar con las segundas (Salman Abdou & Abou Elnasr, 2021: 23[65]). Ambos forman parte del ecosistema *Blockchain* y están transformando la forma en que se percibe el valor en el mundo digital.

Los NFTs constituyen un fenómeno novedoso, pero que ha revolucionado la forma en que se transfieren propiedades digitales únicas (Baker et al., 2022: pp. 2 y 3), como obras de arte, coleccionables, archivos de audio o video, elementos únicos dentro de videojuegos, bienes raíces virtuales, membresías… En medio de la vorágine que ha resultado con su irrupción, la literatura científica ha dado lugar a opiniones muy diversas sobre los NFTs, condensadas por Borri et.al. (2022: p. 2): "Por un lado, se cree que los NFT son un elemento clave del metaverso y la Web3.0 y una revolución en la forma en que se comercializan y monetizan los activos digitales. Por otro lado, los críticos los consideran una moda impulsada por celebridades y una forma de lavar dinero y evitar impuestos". Sin embargo, aún son proyectos en etapas iniciales, por lo que los límites de su potencial e incertidumbre (Taherdoost, 2023: p. 1) aún no son claros. Pero es evidente que las posibilidades de blanquear bienes con las fichas que se estudian existen.

En un estudio en que participó EUROPOL e INTERPOL (Kon, 2021: p. 7) se advirtió sobre el siguiente *modus operandi*: un sujeto que pretende lavar dinero puede generar un NFT anónimo, se lo compra a sí mismo desde una *wallet* anónima donde cuenta con fondos ilícitos, vender el *token* a un tercero y obtener ganancias aparentemente legítimas. Además, el valor del arte —la expresión más frecuente de los NFTs— es muy subjetivo, por lo que se pueden producir burbujas de precios que faciliten el blanqueo (Zheng, 2022: p. 79[66]).

---

embargo, no se comparte ese criterio. Incluso si estos *tokens* representan algo fungible, no significa que ellos, que son código informático único y exclusivo, también lo sean.

[64] Estos "contratos" automáticamente ejecutables funcionan como contenedores digitales, que asignan valores de forma descentralizada y transparente a la cadena de bloques, siendo esencial para los NFTs (Ante, 2021: p. 2).

[65] En el trabajo citado se analiza el caso de las plataformas más populares para adquirir NFTs. Explica el autor que el proceso de compra no se realiza con divisas, sino con criptomonedas y con ello, traslada todos los riesgos criminales que ellas conllevan al espacio de los *tokens* únicos, incluyendo el blanqueo de capitales.

[66] Advierte el investigador que los delincuentes pueden blanquear el dinero incluso con carácter previo a la compra-venta del NFT, invirtiendo en su promoción a través de distintos medios.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

El mundo del arte no es ajeno a este fenómeno criminal, pues este mercado ha ofrecido anonimato y conveniencia para manipular los precios y por eso eficiente para los blanqueadores. Por eso, a partir de la 5ª Directiva antiblanqueo de la Unión[67] ha señalado específicamente a quienes comercian con bienes culturales, como obras de arte, para categorizarlos como sujetos obligados. La normativa indica, en su art. 1.1) c) que se consideran entidades obligadas "las personas que comercien con obras de arte o actúen como intermediarios en el comercio de obras de arte, también cuando lo lleven a cabo galerías de arte y casas de subastas, cuando el importe de la transacción o de una serie de transacciones relacionadas sea igual o superior a 10 000 EUR" y "las personas que almacenen obras de arte, comercien con obras de arte o actúen como intermediarios en el comercio de obras de arte cuando lo lleven a cabo puertos francos, cuando el importe de la transacción o de una serie de transacciones sea igual o superior a 10 000 EUR". En general, el endurecimiento de medidas para prevenir el blanqueo en el contexto artístico y poner el radar sobre su comercio, seguramente ha sido un factor determinante para que los delincuentes buscaran métodos alternativos para lavar el producto de su actividad criminal (Kafteranis et al., 2020: p. 20).

Una preocupación patente en el entorno de los NFTs es la señada por Gámez y Corredor (2023: p. 350): los tecnicismos propios de estos *tokens* han hecho que las plataformas de almacenamiento y gestión que trabajan con ellos operen sin mecanismos antiblanqueo claros, por no haber unicidad en la normativa o regulación que les resulta aplicable. Con el fin de dar solución a esto, en muchos Estados se ha buscado extender aquella relativa a los criptoactivos en general al supuesto de los NFTs, para prevenir el blanqueo de capitales y la financiación del terrorismo (Gupta & Tham, 2019: p. 375). Por ejemplo, Reino Unido ha optado porque su normativa en la materia requiera diligencia debida y similares a toda empresa o profesional que se dedique a los criptoactivos, entendidos como representaciones digitales de valores o derechos contractuales (Skadden et al., 2021: p. 3). Con esta generalidad, la regulación es menos específica pero más inclusiva de las nuevas realidades. De hecho, el propio GAFI (2021: p. 24[68]) reconoce que las normas cripto

[67] 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 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

[68] En un informe más reciente, el mismo Organismo indica que "las autoridades deben adoptar un enfoque funcional y mirar más allá del marketing asociado con los NFT para determinar si el producto o servicio en cuestión califica como VA [activo virtual], VASP [proveedor de servicios de activos virtuales], una institución financiera o una empresa o profesión no financiera designada". En el estudio se realizó una encuesta por jurisdicciones para ver cómo regulaban la utilización de *tokens* no fungibles para blanquear

existentes y las Recomendaciones que ha propuesto pueden cubrir a los NFTs, especialmente cuando se utilizan con fines de pago o de inversión en la práctica. Por otra parte, el Organismo aclara que si el *token* representa un activo financiero ya cubierto por las normas del GAFI, no se entenderían como un activo virtual en sentido estricto, pero igualmente estaría sometido a las medidas antiblanqueo como ese tipo de activo financiero.

El Reglamento MiCA, pese a identificarse como un cuerpo legislativo que actúa sobre los criptoactivos en general, excluye a "los criptoactivos que sean únicos y no fungibles con otros criptoactivos, incluidos las colecciones y el arte digitales". La razón de este descarte es que no son fácilmente canjeables, poseen valores subjetivos y, por tanto, se ven acotados los riesgos para los inversores y el sistema financiero (Considerando 10). Hay quien ha intentado interpretar esta idea de forma extensiva, entendiendo que si los *tokens* en cuestión reciben un uso financiero, se les podría considerar instrumentos regidos por el Reglamento mencionado (Palá Laguna & Canalejas Merín, 2023: p. 4). Los riesgos de blanqueo con NFTs han sido avisados por organismos e instituciones internacionales, por lo que su uso sí concierne riesgos para el sistema financiero[69]. En sede europea, se debía establecer la necesidad de analizar cada caso concreto para ver si la norma desplegaba sus efectos, pero no omitirlos de los NFTs en general. Ahora bien, esta decisión parece sugerir que la pretensión es emitir futuras normativas específicas (Parrondo, 2023: p. 1). Otro indicio de esta idea es el Considerando 15 del Reglamento (UE) 2024/1624: "La creación de mercados de criptoactivos únicos y no fungibles es aún reciente y no ha dado lugar a legislación que regule su funcionamiento. Se está supervisando la evolución de esos mercados y es importante que no genere nuevos riesgos de blanqueo de capitales y financiación del terrorismo que no puedan atenuarse adecuadamente. A más tardar el 30 de diciembre de 2024, la Comisión ha debido de presentar un informe al Parlamento Europeo y al Consejo sobre los últimos avances con

fondos y solo una minoría no les aplicaba en absoluto su marco de prevención contra tal delito y la financiación del terrorismo (GAFI, 2023, pp. 33 y ss.).

[69] Además, el Reglamento MiCA contiene un halo regulatorio bastante amplio, incluso más allá de lo que parece ser totalmente viable en términos prácticos, como lo referente a la supervisión de emisores de criptoactivos y su capacidad de cumplir con los estándares requeridos. Muchos emisores de criptoactivos operan de manera descentralizada o sin una entidad jurídica claramente identificable. Regular estos proyectos, como ocurre con ciertas *stablecoins* algorítmicas o redes DeFi, es complejo porque no existe un único "responsable" a quien supervisar. Además, los emisores que operan fuera del territorio de la Unión pueden eludir el marco regulatorio de MiCA, lo que dificulta su implementación global y su eficacia. No tiene sentido que su ambición normativa no alcanzara a elementos que, si bien tienen serias diferencias, ostentan coincidencias muy notorias con activos virtuales que sí están incluidos dentro de su ámbito de aplicación.

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

respecto a los criptoactivos, incluida una evaluación del desarrollo de los mercados de criptoactivos únicos y no fungibles, el tratamiento normativo adecuado de dichos criptoactivos, la necesidad y la viabilidad de regular a los proveedores de servicios relacionados con criptoactivos únicos y no fungibles. Cuando proceda, la Comisión ha de acompañar dicho informe de una propuesta legislativa". La escasa claridad regulatoria hace que los NFTs sigan estando en una zona gris que necesita ser resuelta para evitar males mayores (Fernández, 2021).

Un informe reciente ha enumerado algunos comportamientos que permiten el lavado de activos con fichas no fungibles (Finanšu Izlūkošanas Dienests, 2020: pp. 10 y ss.): a. Autolavado: el criminal compra un NFT con fondos ilícitos y los transfiere a una cuenta digital. Luego lo vende a un tercero y el dinero obtenido lo mezcla en el sistema económico legítimo. b. *Wash Trading*: los delincuentes realizan transacciones de un *token* de este tipo entre varias billeteras para aumentar su valor progresivamente, generando una falsa impresión entre los inversores. Venden el NFT a un precio inflado, lo que produce ganancias para aquellos sujetos con las que pueden justificar sus fondos ilícitos. c. Fraude Fiscal: quienes tienen deudas fiscales, pueden comprar un NFT y venderlo a una tercera cuenta a un precio significativamente menor, generando una pérdida que compensa las deudas fiscales previas que, incluso, pueden ocultar un fraude fiscal previo. d. *Smurfing*: los delincuentes adquieren una gran cantidad de *tokens* utilizando fondos ilícitos, intercambiándolos entre sus mismas cuentas a la vez que extraen pequeñas cantidades de ganancias mediante el uso de prestadores de servicios de criptomonedas.

Tal como en el caso de las criptomonedas, el blanqueo de capitales con NFTs puede situar estos como medio o como objeto del delito. Si se produce un robo de criptomonedas, el blanqueo de las mismas negociando NFTs, posicionaría a estos como el medio elegido para perpetrar el delito. El objeto, que son las ganancias ilícitas, serían las criptomonedas. Por el contrario, si el delincuente invierte criptomonedas legítimas para adquirir fichas no fungibles valiosas y luego manipula estos activos digitales o los vende falsificados, el objeto del delito se constituiría por estos, pues es lo que se pretende blanquear. Es también el caso, por ejemplo, del *wash trading*. En ambos casos, Chainalysis (2022) insiste en que el análisis de *Blockchain* permitiría rastrear las transacciones de NFTs, analizando las ventas y las direcciones que las financiaron.

V. CONCLUSIONES

A) El blanqueo de capitales se presenta como un delito de referencia, pues requiere la comisión de uno o varios delitos previos de los cuales

resultan los beneficios ilícitos que se introducen o pretenden introducir en el mercado regular. Constituye una amenaza delictiva reconocida y que genera cuantiosos daños a nivel mundial. Las nuevas tecnologías han facilitado la comisión de este delito, en la medida en que incrementa el carácter transnacional que ya caracterizaba a este fenómeno. En especial, las criptomonedas brindan rapidez, opacidad y divisibilidad; lo que las convierte en un medio comisivo particularmente útil. La colocación de los bienes ilícitos, que conforma el eje central del delito de blanqueo, es perfectamente posible en el ecosistema cripto y de forma muy sencilla, pues los delincuentes pueden intercambiar activos virtuales por dinero fiduciario y viceversa. Además de lo expuesto, las criptomonedas permiten el uso de mezcladores y plataformas DeFi que dificultan el rastreo del origen de los fondos. Asimismo, la falta de regulación uniforme a nivel internacional crea zonas grises legales donde los delincuentes operan con mayor impunidad.

B) La tipificación española del delito de blanqueo de capitales, contenida en el art. 301 CP, está alineada con las exigencias internacionales, castigando a quien adquiera, posea, utilice, convierta, transmita bienes o realice cualquier otro acto para encubrir el origen ilícito de los fondos o eludir las consecuencias legales que corresponden. Para algunos autores es una expresión clara de expansionismo punitivo, exigiendo a la labor jurisprudencial un criterio agudizado de acotamiento y concreción de sus elementos. Su extensa y genérica dicción permite entender a las criptomonedas incluidas dentro de los bienes de procedencia ilícita que son el objeto del delito, tanto si se han obtenido directamente ellas con la actividad criminal antecedente, como si se han adquirido a posteriori con las divisas u otros activos generados con la misma. La regulación española también incluye una serie de agravaciones específicas para este delito y admite la posibilidad de que las personas jurídicas puedan responder penalmente por blanqueo de capitales. En torno a esto último, se ha subrayado que los prestadores de servicios de criptoactivos no son las únicas personas jurídicas que puede ser decisivas en el desarrollo del blanqueo, sino también desarrolladores de software, entidades comerciales que acepten pagos en criptomonedas sin implementar mecanismos de prevención o empresas consultoras, auditoras y asesoras legales.

C) El blanqueo de capitales es reconocido por desarrollarse a través de una serie de pasos o etapas secuenciales y las criptomonedas facilitan todas ellas. La colocación puede realizarse con la técnica de *smurfing*, la estratificación con el *chain hopping*, las *cold wallets*, los *mixers*, los centros financieros *off-shore*, etc. Asimismo, las criptomonedas también

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

facilitan todos los delitos previos usualmente relacionados con el blanqueo, lo que genera un serio peligro. Esto confirma que, en efecto, el uso criminal de tales activos virtuales representa un desafío significativo para los sistemas de prevención y persecución penal, al ampliar la capacidad de ocultamiento, anonimato y diversificación de operaciones ilícitas, reforzando así la necesidad de adaptar los marcos normativos y los mecanismos de control a las nuevas tecnologías financieras.

D) La modalidad imprudente es admisible en la tipificación española del blanqueo de capitales, la cual ha sido usualmente aplicada a los "muleros"; es decir, aquellas personas que actúan como mediadores activos entre dos partes que quieren hacer una transacción: A envía dinero al mulero y este lo transmite a B. Muchas de estas personas actúan sin tener motivaciones criminales pero su falta de diligencia debida puede suponer la atribución de responsabilidad penal. Por la asistencia financiera que suponen en casos de blanqueo de capitales y la dificultad que añaden a la persecución del delito, los organismos supervisores españoles han diseñado nuevos medios para comunicar cuentas y transacciones sospechosas de actuar como "mulas". Esta evolución del sistema para avanzar en materia antiblanqueo debe perfeccionarse y precisarse cuando intervienen criptomonedas, que sirven a estos sujetos por su pseudonimato/anonimato y rapidez. El fenómeno de las "mulas" mediante criptoactivos es difícil de rastrear, pero puede limitarse reforzando la regulación sobre prestadores de servicios cripto como sujetos obligados. Pero también puede ser útil implementar medidas técnico-prácticas específicas como el empleo de modelos de análisis predictivo con algoritmos de aprendizaje y modelos de regresión logística, árbol de decisión y métodos de ensamble. Se han consultado estudios que reseñan estos potenciales progresos, pero aún hay limitaciones por solventar.

E) Las ICOs son mecanismos para financiar proyectos iniciales con la emisión de *tokens*, en este caso criptográficos. Tiene grandes ventajas financieras, sobre todo la reducción de costos y la amplia accesibilidad de estas plataformas. No obstante, su falta de regulación y la imprecisión de sus *white papers* (suelen carecer de aspectos técnicos, financieros o legales relevantes) los convierte en vehículos potenciales, no solo para las estafas, sino también para el blanqueo de capitales. Aunque el Reglamento MiCA en Europa establece ciertos requisitos mínimos, muchas ICOs siguen operando en entornos opacos, favoreciendo el anonimato y la elusión normativa. Por ello, se recomienda extender las obligaciones de diligencia debida y KYC a sus operadores para prevenir usos delictivos. Distinto es el caso de la autocustodia de criptomonedas, donde no interviene ningún sujeto profesional obligado por la normativa

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

antiblanqueo. Este supuesto es limitadamente regulable, pero cuando las billeteras autocustodiadas interactúen con otras que sí se gestionen por intermediarios que cumplen medidas de diligencia debida y la regla de viaje, se podrán obtener datos de partida para emprender labores de investigación. Este contraste evidencia que la eficacia en la prevención y tratamiento del blanqueo de capitales en el ámbito cripto depende en gran medida del grado de intervención de sujetos obligados, razón por la que ha sido de máxima atención regulatoria en los últimos años. Pero también demuestra que no se trata solo de reforzar el marco normativo, sino que requiere el desarrollo de herramientas tecnológicas y colaboraciones interinstitucionales, incluso cuando se trate de entornos no custodiados por sujetos obligados.

F) Se ha estudiado el caso de las tarjetas de débito y crédito vinculadas a carteras de criptomonedas, el *proof-of-burn* y la vinculación entre criptomonedas y NFTs y, en conjunto, remarcan que todas las manifestaciones del ámbito cripto no pueden ser abordadas en categorías generales ni con medidas reactivas globales. Es necesario un enfoque granular y aplicado al uso real y funcional de cada tecnología y su integración en el delito. La fragmentación regulatoria del Reglamento MiCA parece indicar que se avecinan futuras normativas específicas —por ejemplo, para el caso de los NFTs—, lo que también plantea problemas jurídicos y operativos. El blanqueo de capitales exige anticipación y coherencia regulatoria y la espera sostenida por nuevas normativas y la dispersión que esto puede suponer, supondría un marco complejo y de difícil aplicación, especialmente si no se definen arquitecturas legales que permitan su integración en la práctica.

VI. REFERENCIAS CONSULTADAS

1. *Referencias bibliográficas*

Abdul, M., Zolkafil, S. & Mustapha, S. (2022). The money mule red flags in anti-money laundering transaction monitoring investigation. *International Journal of Business and Economy*, vol. 4, núm. 1.

Aggarwal, N. & Floridi, L. (2019). The opportunities and challenges of blockchain in the fight against government corruption. *19th General Activity Report, Grupo de Estados contra la Corrupción*.

Albanese, J. & Artello, K. (2019). The behavior of corruption: an empirical typology of public corruption by objective & method. *Criminology, Criminal Justice, Law & Society*, vol. 20, núm. 1.

Albrecht, C., McKay, K., Hawkins, S. & Morales, V. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, vol. 22, núm. 2.

Alldridge, P. (2001). The moral limits of the crime of money laundering. *Buffalo Criminal Law Review*, vol. 5, núm. 1.

Alnasaa, M., Gueorguiev, N., Honda, J., Imamoglu, E., Mauro, P., Primus, K. & Rozhkov, D. (2022). Crypto, corruption, and capital controls: cross-country correlations. *International Monetary Fund Working Papers*, núm. 22/60.

Amrani, H. (2012). The development of anti-money laundering regime: challenging issues to sovereignty, jurisdiction, law enforcement, and their implications on the effectiveness in countering money laundering. *Erasmus University Rotterdam*.

Angurem, R., García Alcorta, J., García Calvo, L., Hernández García, D. & Valdeolivas, E. (2023). La regulación de los criptoactivos en el marco internacional y europeo en curso. *Revista de Estabilidad Financiera*, núm. 44.

Ante, L. (2021). Non-fungible token (NFT) markets on the Ethereum blockchain: temporal development, cointegration and interrelations. *Blockchain Research Lab Working Paper Series*, núm. 22.

Aránguez Sánchez, C. (2000). El delito de blanqueo de capitales. *Marcial Pons*.

Arman, M. & Nendi, I. (2023). Money laundering: a three step secret game. *Journal of Social Science*, núm. 2.

Austrac. (2024). Combating the exploitation of International Students as Money Mules. *Guía del Crimen Financiero*.

Bacigalupo, S. & Bajo, M. (2010). Derecho penal económico. *Editorial Universitaria Ramón Areces*.

Baker, B., Pizzo, A. & Su, Y. (2022). Non-fungible tokens: a research primer and implications for sport management. *Sports Innovation Journal*.

Barrera, J. & Hessdörfer, A.. (2012). El engaño como conducta típica en la defraudación tributaria: puntos de contacto y asimetrías entre el régimen infraccional y penal. *Revista de Derecho de la Universidad de Montevideo*, año 11, núm. 21.

Blanco Cordero, I. (2011). El delito fiscal como actividad delictiva previa del blanqueo de capitales. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13-01.

Blanco Cordero, I. (2021). El delito de blanqueo de capitales. *Editorial Aranzadi*.

Blanco Escinosa, L. (2023). NFT: ¿Se expande y profundiza el universo criptofinanciero? *Cofin Habana*, vol. 17, núm. 2.

Bolea Bardón, C. (2016). El delito de corrupción privada: bien jurídico y ratio legis. En *Prevención y tratamiento punitivo de la corrupción en la contratación pública y privada* (coord. L. Graffe González). Editorial Dykinson.

Borri, N., Liu, Y. & Tsyvinski, A. (2022). The economics of non-fungible tokens. *SSRN Electronic Journal*, enero 2022.

Brownworth, A., Durfee, J., Junho, M. & Martin, A. (2024). Regulating decentralized systems: evidence from sanctions on Tornado Cash. *SNB Working Papers*, núm. 9.

Caba Tena, A. (2022). La prueba del delito de "blanqueo de capitales" en la jurisprudencia más reciente de la Sala Segunda de lo Penal del Tribunal Supremo. *ElDerecho*, Lefebvre, 08 de febrero, s/p.

Camacho Belmonte, M. (2017). Responsabilidad del asesor fiscal ante el blanqueo de capitales. *Tribuna y Boletín de la FICP*, núm. 2.

Cámara Barroso, M. (2016). El "delito fiscal". *Revista de Contabilidad y Tributación. CEF*, núm. 397.
Camassa, C. (2023). Legal NLP meets MICAR: advancing the analysis of crypto white papers. *NLLP*.
Campino, J., Brochado, A. & Rosa, A. (2022). Initial Coin Offerings (ICOs): why do they succeed? *Financial Innovation*, vol. 8, núm. 17.
Carballo, B. (2023). El tipo penal del blanqueo de capitales: una exigencia económica que ha perdido los límites. *El Derecho*.
Carbajo Gascón, F. (2012). Corrupción en el sector privado (I): la corrupción privada y el derecho privado patrimonial. *Iustitia*, núm. 10.
Carpio, J. (2018). Bitcoin y criptoeconomía: ficción y futuro. *Koyuntura*, núm. 73, año 9.
Cassella, S. (2018). Toward a new model of money laundering: is the 'placement, layering, integration' model obsolete? *Journal of Money Laundering Control*.
Castelló Nicás, N, (2022). Principio de intervención mínima versus adecuación social, tolerancia social, e insignificancia en delitos de corrupción privada. *Cuadernos de Política Criminal*, segunda época, núm. 137.
Castro Moreno, A. (2017). Nuevas tendencias sobre el delito de blanqueo: ¿anteblanqueo? Delito fiscal, blanqueo de capitales y regularización tributaria. En *Corrupción y delito: aspectos de derecho penal español y desde la perspectiva comparada*. Editorial Dykinson.
Cevallos Pachacama, I. (2024). Lavado de activos a través de monedas virtuales, una perspectiva jurídica y académica. *Mentor. Revista de Investigación Educativa y Deportiva*, vol. *3*, núm. 8.
Chanjan Document, R., Solis, E. & Puchuri, F. (2018). Sistema de justicia, delitos de corrupción y lavado de activos. *Pontificia Universidad Católica del Perú y National Endowment for Democracy*.
De Andrés, P., Arroyo, D., Correia, R. & Rezola, A. (2022). Challenges of the market for initial coin offerings. *International Review of Financial Analysis, núm. 79*.
De la Cuerda Martín, M. (2017). El fraude fiscal como delito previo al blanqueo de capitales. *Gabilex*, núm. 12.
De la Cuesta Arzamendi, J. & Blanco Cordero, I. (2017). Corrupción. En Paz Lloria y Francisco Boix (coords.), *Diccionario de Derecho Penal Económico*.
De la Mata Barranco, N. (2016). El delito fiscal del art. 305 CP después de las reformas de 2010, 2012 y 2015: algunas cuestiones, viejas y nuevas, todavía controvertida. *Revista General de Derecho Penal,* núm. 26.
De Mosteyrín Sampalo, R. (2016). El delito de blanqueo de capitales a la luz de la normativa internacional sobre la materia (1). *Anuario de Derecho Penal y Ciencias Penales*, tomo 69, fasc. 1.
De Vicente, R. (2024). Vademécum de Derecho Penal. *Editorial Tirant Lo Blanch*, 7ª Edición.
Delgado Sancho, C.D. (2023). Blanqueo de capitales y financiación el terrorismo. Aspectos jurídicos del blanqueo de capitales y financiación del terrorismo en sus vertientes penal y administrativa. *Editorial Marcial Pons*.
Del Monaco, S. (2020). Money Mules and Tumblers. Money Laundering During the Cryptocurrency Era. *Ricerche giuridiche*, vol. 9, núm. 2.

Departamento del Tesoro de los Estados Unidos (2023). Illicit Finance Risk Assessment of Decentralized Finance. Abril.

Domínguez Martínez, J. (2023). La tributación de las criptomonedas: aspectos básicos. *Edufinet*, núm. 9.

El-Banna, M., Khafagy, M., & El Kadi, H. (2020). Smurf Detector: a detection technique of criminal entities involved in money laundering. En *International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)*.

Elliptic (2022). The state of cross-chain crime. *Elliptic Cross-Chain Report*.

Elsayed, S. (2023). Cryptocurrencies, corruption and organised crime. *U4 Helpdesk Answer*, Anti-Corruption Resource Centre y Transparency International.

Erinle, Y., Kethepalli, Y., Feng, Y., & Xu, J. (2025). SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets. *Computer Networks*, núm. 273.

Essaghoolian, N. (2019). Initial Coin Offerings: Emerging Technology's Fundraising Innovation. *U.C.L.A. Law Review*, núm. 66.

Europol (2023). One of the darkweb's largest cryptocurrency laundromats washed out [Nota de prensa], 15 de marzo, s/p.

Fabián Caparrós, E. (2010). Algunas observaciones sobre el blanqueo imprudente de capitales (aspectos doctrinales y jurisprudenciales). *Iustitia*, núm. 8.

Fernández, C. (2021). Desmitificando los Tokens No Fungibles o NFT. *Diario La Ley*, s/p.

Fernández Bermejo, D. (2020). Análisis normativo de la regularización penal tributaria como excusa absolutoria. *Anuario de Derecho Penal y Ciencias Penales*, tomo 73, fasc. 1.

Fernández Cruz, J. (2005). Estudio político criminal sobre el tipo imprudente de legalización de capitales. *Revista de Derecho*, núm. 26.

Fernández Teruelo, J. (2019). Responsabilidad penal de las personas jurídicas: El contenido de las obligaciones de supervisión, organización, vigilancia y control referidas en el art. 31 bis 1. b) del Código Penal español. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 21-03.

Figueroa, Castillo, V., Villacreses Parrales, C., Chóez Calle, J., Barreto Pin, J., & Maldonado Zúñiga, K. (2021). El blockchain y los contratos inteligentes; una forma de reducir la corrupción. *Serie Científica de la Universidad de las Ciencias Informáticas*, vol. 14, núm. 5.

Forgang, G. (2019). Money Laundering Through Cryptocurrencies. En *Economic Crime Forensics Capstones*.

Fu, X., Wnag, H., & Shi, P. (2021). A survey of Blockchain consensus algorithms: mechanism, design and applications. *Science China Information Sciences*, vol. 64.

Gámez, M., & Corredor, J. (2023). NFT (token no fungibles) y sus implicaciones en el mercado de valores. *Derecho PUCP*, núm. 90.

Gomes Pereira, P., & Fontana, A. (2019). Using Money Laundering Investigations to Fight Corruption in Developing Countries: Domestic obstacles and strategies to overcome them. Centro Internacional para la Recuperación de Activos, *Working Papers Series*, núm. 14.

González Quinzán, Y. (2023). Normativa internacional sobre el blanqueo: más allá de las directivas de la Unión Europea. *Cadernos de Dereito Actual*, núm. 22.

González Rus, J.J. (2024). Delitos contra el patrimonio y el Orden Socioeconómico. En *Sistema de Derecho Penal. Parte especial* (dir. L. Morillas Cueva).

Gran, B., Kieseberg, K., Çulha, C., Koelbing, M., & Simos, D. (2023). A Mathematical Approach on the Use of Integer Partitions for Smurfing in Cryptocurrencies. En *Mathematical Research for Blockchain Economy* [Paper].

Guidara, A. (2022). Cryptocurrency and money laundering: A literature review. *Corporate Law & Governance Review*, vol. 4, núm. 2.

Gupta, P., & Tham, T. M. (2019). Fintech. The New DNA of Financial Services. Research Collection Lee Kong Chian School Of Business.

Hellvig, R., & Blanaru, C. (2023). Impact of globalization on money laundering. *SEA — Practical Application of Science*, vol. 11, núm. 32.

Hinojal Fraile, A. (2023). Criptomonedas y blanqueo de capitales. *Lógos: Revista Científica del Centro Universitario de la Guardia Civil*, junio 2023.

Hrytsai, S. (2023). Cryptocurrency in the declarations of Government Officials: A toolkit for money laundering (trends and experience of counteraction by the example of Ukraine). *Access to Justice in Eastern Europe*.

Ibrahimi, A., & Arifi, B. (2022). Corruption and Cryptocurrency. Blockchains as corruption tools. *Academicus International Scientific Journal*, núm. 26.

Jabotinsky, H. & Lavi, M. (2022). Speak Out: Verifying and Unmasking Cryptocurrency User Identity. *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 32, núm. 3.

Jaroucheh, Z., & Ghaleb, B. (2023). Crypto Assets Custody: Taxonomy, Components, and Open Challenges. En *IEEE International Conference on Blockchain and Cryptocurrency*.

Jiménez García, F. (2016). Blanqueo de capitales y Derecho internacional. *Eunomía. Revista en Cultura de la Legalidad*, núm. 10.

Kafteranis, D., Unozkan, H., & Turksen, U. (2023). Know your NFTs: Compliance and enforcement challenges in trading of non-fungible tokens. *International Journal of Law in Changing World*, núm. 2, Número especial: NFTs and The Legal Landscape.

Karantias, K., Kiayias, A., & Zindros, D. (2020). Proof-of-Burn. En *24th International Conference on Financial Cryptography and Data Security*.

Kerzic, K. (2022). Using predictive analytics for money mule detection on a cryptocurrency exchange. Master Program in Information Management, Nova IMS.

Kim, D., Huseyin, M., & Ryu, D. (2021). Are suspicious activity reporting requirements for cryptocurrency exchanges effective? *Financial Innovation*, núm. 78.

Koelbing, M., Kieseberg, K., Çulha, C., Garn, B. & Simos, D. (2024). Modelling smurfing patterns in cryptocurrencies with integer partitions. *IET Blockchain*.

Kon, M. (2021). NFTs The Ultimate Money Laundering tool??? Basel Institute on Governance, EUROPOL e INTERPOL.

Kublen, L. (2015). Cuestiones fundamentales del delito de fraude fiscal. Traducción de B. Cruz Márquez y J. L. Fuentes Osorio. Editorial Marcial Pons.

Labaqui, I. (2003). Las causas de la corrupción: un estudio comparado. *Colección*, año 9, núm. 14.

Lascuraín Sánchez, J. A. (2018). Blanqueo de capitales. En *Derecho Penal Económico y de la Empresa* (N. de la Mata Barranco, J. Dopico Gómez-Aller, J. A. Lascuraín Sánchez y A. Nieto Martín, aut.).

Lawrence, D. (2022). The Dark Side of Cryptocurrency Hardware Wallets. *ACFE*, Blog, enero 2022.

Levi, M., & Soudijn, M. (2020). Understanding the Laundering of Organized Crime Money. *The University of Chicago Press Journals*, vol. 49.

Manninen, H. (2023). The Anti-money Laundering Challenges of FinTech and Cryptocurrencies. *Nordic Journal of Legal Studies*, núm. 1.

Manso Porto, T. (2011). El blanqueo de capitales entre la dogmática y la Política criminal internacional: Resultados desde una perspectiva de Derecho comparado. *Estudios Penales y Criminológicos*, vol. 41.

Matallín Evangelio, A. (2018). Blanqueo de capitales y principios penales. *Teorder*, núm. 24.

Martiñón, R. (2012). Fraude fiscal. *Eunomía. Revista en Cultura de la Legalidad*, núm. 2.

Martín Sagrado, O. (2018). La determinación del bien jurídico protegido por el delito de blanqueo de capitales y el autoblanqueo. Un debate que no cesa. *Boletín del Ministerio de Justicia*, año 72, núm. 2206.

Mendoza Llamacponcca, F. (2013-2014). El delito fuente en el lavado de activos. En *Temas de Derecho Penal Económico: Empresa y Compliance. Anuario de Derecho Penal*.

Miranzo Díaz, J. (2018). Causas y efectos de la corrupción en las sociedades democráticas. *Revista de la Escuela Jacobea de Posgrado*, núm. 14.

Molina Mansilla, C. (2007). El delito básico de blanqueo de capitales del artículo 301 del Código Penal. *Diario La Ley*, s/p.

Momtaz, P. (2020). Initial Coin Offerings. *PLoS ONE*, vol. 15, núm. 5.

Monteiro Lima, A., & Márcio, A. (2021). Lavado de dinero en el entorno cibernético y criptoactivos en el hemisferio. *Hemisferio Revista del Colegio Interamericano de Defensa*, núm. 7.

Monteverde Valero, E. (2021). Corrupción como delito. En N. González (Ed.), *Covid-19 y su circunstancia. Una visión jurídica plural de la pandemia*. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas e Instituto de Estudios Constitucionales del Estado de Querétaro, 1ª Edición.

Mooij, A. (2024). Money Laundering and Financing of Terrorism via the Metaverse. En *Regulating the Metaverse Economy*. Springer.

Morillas Cueva, L. (2013). Aspectos dogmáticos y político-criminales del delito de blanqueo de capitales. *Revista Foro FICO*, núm. 2.

Morillas Cueva, L. (2023). La difícil concreción del concepto y alcance del término corrupción. En *Corrupción privada, transparencia y gestión pública*. Editorial Dykinson.

Moxotó, A.C., Melo, P., & Soukiazis, E. (2021). Initial Coin Offering (ICO): a systematic review of the literature. En *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Myint, U. (2000). Corruption: Causes, consequences and cures. *Asia-Pacific Development Journal*, vol. 7, núm. 2.

Navarro Cardoso, N. (2019). Criptomonedas (en especial, bitcóin) y blanqueo de dinero. *Revista electrónica de ciencia penal y criminología*, núm. 21.

Nieto Martín, A., & García-Moreno, B. (2021). Criptomonedas y derecho penal: más allá del blanqueo de capitales. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 23.

Olmedo Cardenete, M. (2024). Delitos contra el patrimonio y el orden socioeconómico (XIV): La receptación y el blanqueo de capitales. En *Sistema de Derecho penal. Parte especial*. L. Morillas Cueva (Dir.).

Oportot Campillay, R. (2024). Millonario desfalco en Algarrobo provoca recortes en beneficios sociales. *Doble Espacio. Revista de la Escuela de Periodismo de la Universidad de Chile*.

Palá Laguna, R., & Canalejas Merín, J. (2023, junio). A qué criptoactivos no se aplicará el Reglamento MiCA. *Revista Mercantil Gómez-Acebo & Pombo*.

Parrondo, L. (2009). *El blanqueo de capitales: delito autónomo y principio de tipicidad*. Editorial Dykinson.

Peres, R., Schreier, M., Schweidel, D. & Sorescu, A. (2022). Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing*, núm. 40.

Peters, A. (2018). Corrupción y derechos humanos. En C. Tablante y M. Morales (Eds.), *Impacto de la corrupción en los derechos humanos*. Instituto de Estudios Constitucionales del Estado de Querétaro.

Pickles, R. (2021). 'Money Mules': Exploited Victims or Collaborators in Organised Crime? *Irish Probation Journal*, vol. 18.

Policía Metropolitana del Reino Unido. (2024). *The little book of crypto crime*.

Prendi, L., Borakaj, D., & Prendi, K. (2023). The new money laundering machine through cryptocurrency: Current and future public governance challenges. *Corporate Law & Governance Review*, vol. 5, núm. 2.

Proaño Alcívar, D. (2024). Desmitificando la no fungibilidad de los NFT. *USFQ Law Review*, vol. 11, núm. 1.

Real Academia Española. (2014). *Diccionario de la lengua española* (23.ª ed.).

Reinoso Martínez, F. (2020). *Prontuario jurisprudencial del delito de blanqueo de capitales*. Editorial Dykinson.

Ribeiro Pereira, R. (2021). *A machine learning approach to money laundering detection inspired by GANs*. Repositório Aberto da Universidade do Porto.

Rodinko, M., Oliynykov, R. & Nastenko, A. (2024). Decentralized Proof-of-Burn auction for secure cryptocurrency upgrade. *Blockchain: Research and Applications*, vol. 5, núm. 1.

Saldaña Taboada, P. (2017). ¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado. *El Criminalista Digital. Papeles de Criminología,* núm. 6.

Salman Abdou, A., & Abou Elnasr, R. (2021). Prospects of investment in digital art: Case of Ethereum and Non-Fungible Token (NFT). Economics and Law, vol. 3, núm. 2.

Sánchez Bernal, J. (2010). La corrupción en el sector privado: debate en torno a su inclusión en el Código Penal. Cuadernos del Tomás, núm. 2.

Sánchez Robert, M. (2016). La tipificación del delito de blanqueo de capitales en los ordenamientos jurídicos español y alemán. El expansionismo del derecho penal y el autoblanqueo. *Cuadernos de Política Criminal*, núm. 119.

Sánchez Robert, M. (2021). Blanqueo de capitales y enriquecimiento ilícito en el ámbito de la corrupción política. En L. Morillas Cueva (Dir.), *Respuestas jurídicas frente a la corrupción política*. Editorial Dykinson.

Sánchez Robert, M. (2023). Técnicas jurídico-privadas para el encubrimiento de operaciones de blanqueo. En L. Morillas Cueva (Dir.), *Corrupción privada, transparencia y gestión pública*. Editorial Dykinson.

Sánchez Seco, J. (2013). Blanqueo de capitales. Motivos que justifican la existencia de la regulación de prevención del blanqueo de capitales. En *VII Curso de Alta Especialización en Fiscalidad Financiera*.

Sanz-Bas, D., Del Rosal, R., Náñez, J., & Echarte, M. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws*, vol. 10, núm. 3.

Schneider, F., & Windischbauer, G. (2010). Money Laundering: Some Facts. *Economics of Security Working Paper*, núm. 25.

Scott, D. (1995). Money Laundering and International Efforts to Fight It. Public Policy for the Private Sector, núm. 48. Banco Mundial.

Shadrooh, S., & Nørvåg, K. (2024). SMoTeF: Smurf money laundering detection using temporal-order and flow analysis. *Applied Intelligence*, núm. 54.

Souto, M.A. (2024). Blanqueo de monedas virtuales y criptoactivos en la UE desde las Directivas de 2018 hasta los Reglamentos de 2023. En M. García, V. Rodríguez, M. Díaz y García Conlledo, & D. Luzón Peña (Dirs.), Libro homenaje al profesor Javier de Vicente Remesal por su 70.º aniversario. Fundación Internacional de Ciencias Penales.

Souto, M.A. (2022). COVID-19 y comisión del delito de blanqueo de dinero mediante las nuevas tecnologías. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 24-28.

Souto, M.A. (2021). El delito de blanqueo de dinero o la legitimación de ganancias en Bolivia y su necesaria interpretación desde una perspectiva constitucional. *Revista Jurídica Derecho*, vol. 10, núm. 14.

Souto, M.A. (2022). La comisión imprudente del blanqueo. *Revista Penal México*, núm. 21.

Starnini, M., Tsourakakis, C., Zamanipour, M., Panisson, A., Allasia, G., Fornasiero, J., Li Puma, G., Ricci, F., Ronchiadin, S., Ugrinoska, S., Varetto, E., & Moncalvo, F. (2021). *Smurf-Based Anti-money Laundering in Time-Evolving Transaction Networks*. En G. De Francisci Morales, C. Perlich, N. Ruchansky, N. Kourtellis, E. Baralis, & F. Bonchi (Eds.), Machine Learning and Knowledge Discovery in Databases. Applied Data Science Track.

Subashi, E. (2024). Cryptocurrencies and Money Laundering. *Balkan Journal of Interdisciplinary Research,* vol. 10, núm. 1.

Taherdoost, H. (2023). Non-Fungible Tokens (NFT): A Systematic Review. *Information*, vol. 14, núm. 26.

Taylor, M., Ho-Yong, S., Zainol, Z., & Sheikh, A. (2022). A comprehensive forensic preservation methodology for crypto wallets. *Forensic Science International: Digital Investigation,* vol. 42 y 43.

Thommandru, A. (2023). Smurfing in electronic banking: A legal investigation of the potential for transnational money laundering. *International Journal of Legal Information*, vol. 51, núm. 1.

Unger, B. (2007). The scale and impacts of money laundering. Elgar Online.

Unger, B. (2017). Offshore activities and money laundering: Recent findings and challenges. Parlamento Europeo.

Van Koningsveld, J. (2013). Money laundering "You don't see it, until you understand it": Rethinking the stages of the money laundering process to make enforcement more effective. En *Research Handbook on Money Laundering*. Edward Elgar Publishing.

Vázquez Iruzubieta, C. (2015). De la receptación y el blanqueo de capitales. *Comentarios al Código Penal*. Editorial vLex.

Vidales Rodríguez, C. (2015). Régimen jurídico de la prevención y represión del blanqueo de capitales. Editorial Tirant lo Blanch.

Vieira Dos Santos, J. (2020). Regulação dos Criptoativos. *Cadernos do Mercado de Valores Mobiliários*, núm. 64.

Wagner, M. (2023). Democratic Rep says self-custody wallets should have federal digital identities. Blockwork.

Yazid bin Zul Kepli, M., & Adeniyu Nasir, A. (2016). Money laundering: Análisis on the placement methods. International Journal of Business, Economics and Law, vol. 11, núm. 5.

Zeldin, M. (1994). Money laundering: Legal issues. En R. C. Effros (Ed.), *Current legal issues affecting central Banks,* vol. 2.

Zheng, Y. (2022). The research of NFT money laundering risks and regulatory measures. *Frontiers in Business Economics and Management*, vol. 6, núm. 3.

2. *Referencias jurisprudenciales*

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 279/2013, de 6 de marzo de 2013. ECLI ES:TS: 2013:1486

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 224/2024, de 7 de marzo de 2024. ECLI ES:TS: 2024:1337

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 974/2012, de 5 de diciembre de 2012. ECLI: ES:TS: 2012:8701.

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 277/2018, de 8 de junio de 2018. ECLI: ES:TS: 2018:2056

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 156/2011, de 21 de marzo de 2011. ECLI: ES:TS: 2011:1864

STS 139/2009

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 139/2009, de 24 de febrero de 2009. ECLI: ES:TS: 2009:609

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 408/2015, de 8 de julio de 2015. ECLI: ES:TS: 2015:3504

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 67/2006, de 7 de febrero de 2006. ECLI: ES:TS: 2006:503

Estudios de Deusto. Revista de Derecho Público
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062
https://doi.org/10.18543/ed.3751 • http://www.revista-estudios.deusto.es/

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 506/2015, de 27 de julio de 2015. ECLI: ES:TS: 2015:3520

TRIBUNAL SUPREMO. Sala Segunda (Penal). Nº Resolución 412/2014, de 20 de mayo de 2014. ECLI: ES:TS: 2014:2110

3. *Referencias legislativas*

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado, núm. 281,* de 24 de noviembre de 1995.

Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego. *Boletín Oficial del Estado, núm. 164*, de 10 de julio de 2021.

Real Decreto 249/2023, de 4 de abril, por el que se modifican el Reglamento General de Desarrollo de la Ley 58/2003, de 17 de diciembre, General Tributaria, en materia de revisión en vía administrativa, aprobado por el Real Decreto 520/2005, de 13 de mayo; el Reglamento General de Recaudación, aprobado por el Real Decreto 939/2005, de 29 de julio; el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio; el Reglamento del Impuesto sobre Sucesiones y Donaciones, aprobado por el Real Decreto 1629/1991, de 8 de noviembre; el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre; el Reglamento del Impuesto sobre la Renta de las Personas Físicas, aprobado por el Real Decreto 439/2007, de 30 de marzo, y el Reglamento del Impuesto sobre Sociedades, aprobado por el Real Decreto 634/2015, de 10 de julio. *Boletín Oficial del Estado, núm. 81*, de 5 de abril de 2023.

Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a la información que acompaña a las transferencias de fondos y de determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849. *Diario Oficial de la Unión Europea, núm. 150*, de 9 de junio de 2023.

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937. *Diario Oficial de la Unión Europea, núm. 150,* de 9 de junio de 2023.

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. *Diario Oficial de la Unión Europea, núm. 1624*, de 19 de junio de 2024.

4. *Otros documentos y webgrafía*

Abogacía Española (2022). El Tribunal Supremo acota las conductas que pueden juzgarse por blanqueo de capitales. *Consejo General*, 24 de marzo.

AML UAE (2023). Peeling back the layers: how layering techniques are used in money laundering.
Chainalysis (2022). Crime and NFTs: Chainalysis detects significant wash trading and some NFT money laundering in this emerging asset class. *Informe*, febrero, s/p.
Cointelegraph Research (2024). Cierre de Samourai Wallet: implicaciones para la privacidad y autocustodia. *Cointelegraph*, 14 de junio.
ESMA (2017). ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs). Declaración Oficial.
Europol (2019). Uso de mulas de dinero. Infografía, noviembre.
EY (2022). NFTs: El auge del arte digital. Diciembre.
Financial Intelligence Centre de Sudáfrica (2024). Financial crime insights: Money laundering risks associated with money mules. Reporte, vol. 1, junio.
Finanšu Izlūkošanas Dienests (2022). Money Laundering, terrorism and proliferation financing risks of NFTs. Estudio de análisis estratégico.
Fiscalía de Chile (2024). URAC formaliza a ex alcalde de Algarrobo y otros siete imputados por lavado de activos. Sala de Prensa, 10/06/2024.
Fiscalía de los Estados Unidos (2024). Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses [Comunicado de Prensa], 24 de abril, s/p.
Floriane, B. (2019). Review du Samouraï Wallet. *Journal du Coin*, s/p.
GAFI (2010). Corruption. A reference guide and information note on the use of the FATF Recommendations to support the fight against corruption.
GAFI (2011). Laundering the Proceeds of Corruption. Reporte.
GAFI (2019). Virtual assets and virtual asset service providers. Guía.
GAFI (2020). Informe del GAFI. Activos Virtuales. Señales de alerta de LD/FT.
GAFI (2023). Countering Ransomware Financing. Reporte.
KPMG (2024). Money Mules: FinCrime's Trojan Horse Unveiled. Informe, septiembre 2024.
Kryptomat (s/f). A Beginner's Guide to Analysing Crypto White Papers Before Buying.
Ministerio del Interior de España (2024). La Guardia Civil desarticula una organización que robaba coches de alta gama para venderlos y blanquear el dinero con criptomonedas [Nota de prensa].
Palazzo, M. (2024, 06 de junio). Ex alcalde chileno fue procesado por robar fondos públicos para comprar criptomonedas y casas en Estados Unidos [Nota de prensa]. *Infobae*.
SEPBLAC. (2024 a). Preguntas frecuentes sobre el nuevo sistema de comunicación por indicio de cuentas Mula.
SEPBLAC. (2024 b). Comunicación agregada de Cuentas Mula.
Skadden, Arps, Slate, Meagher & Flom. (15 de junio de 2021). Regulatory Approaches to Nonfungible Tokens in the EU and UK [Memorándum].
World Federation of Exchanges. (2024). Crypto-asset custody: A blueprint for regulatory and operational excellence.