Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Artículo de Investigación

BLANQUEO DE CAPITALES MEDIANTE CRIPTOACTIVOS: EFICACIA REGULATORIA Y BRECHA ENTRE TRAZABILIDAD TECNOLÓGICA Y ATRIBUCIÓN JURÍDICA EN LA UNIÓN EUROPEA Y ESTADOS UNIDOS

Benjamín Garcinuño Roldán
Doctorando en la Escuela Internacional de Doctorado de la UNED (EIDUNED), Guardia Civil, abogado ejerciente en el Ilustre Colegio de Abogados de Córdoba.
Máster en Seguridad, Licenciatura en Derecho
bgarcinun2@alumno.uned.es
https://orcid.org/0009-0005-6923-1004

Recibido 25/02/2026
Aceptado 02/06/2026
Publicado 30/06/2026

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Cita recomendada: Garcinuño, B. (2026). Blanqueo de capitales mediante criptoactivos: eficacia regulatoria y brecha entre trazabilidad tecnológica y atribución jurídica en la Unión Europea y Estados Unidos. *Revista Logos Guardia Civil*, 4(2), pp. 215-252. https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

DEDICATORIA

A Mariam, por confiar en mí,
y por alimentar los pájaros de mi cabeza.
He de recordarle que el sol sigue brillando, aunque no lo mire.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

BLANQUEO DE CAPITALES MEDIANTE CRIPTOACTIVOS: EFICACIA REGULATORIA Y BRECHA ENTRE TRAZABILIDAD TECNOLÓGICA Y ATRIBUCIÓN JURÍDICA EN LA UNIÓN EUROPEA Y ESTADOS UNIDOS

Resumen: El blanqueo de capitales es un fenómeno dinámico cuya evolución está vinculada al entorno económico internacional. Los métodos de blanqueo de capitales ilícitos generan nuevos desafíos regulatorios y operativos a las autoridades y a las entidades financieras, en gran medida impulsados por el desarrollo de la tecnología. Con el uso de ciertas tecnologías recientes, generan un entorno de seudonimidad, el cual trasciende su naturaleza meramente técnica. Este rasgo opera como un instrumento estratégico para las organizaciones y grupos criminales (OC) que buscan sofisticar sus esquemas de blanqueo, permitiendo la ocultación de la trazabilidad y la consecuencia de los daños subyacentes**.** El presente artículo analiza críticamente la problemática del blanqueo de fondos ilícitos mediante criptoactivos por parte de las OC y las diversas estrategias que emplean los OC para ocultar su trazabilidad e identidad. En primer lugar, se examinan de manera sistemática los instrumentos internacionales como son la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) en relación

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

con el sistema de persecución y prevención del blanqueo de fondos ilícitos mediante criptoactivos. A partir de este marco internacional, el presente trabajo se articula en torno a un análisis comparativo del marco legislativo, sustancialmente diferentes frente al blanqueo de capitales mediante criptoactivos en los Estados Unidos (EE. UU) y la Unión Europea (UE). El presente estudio no se limita a una aproximación descriptiva del fenómeno, sino que pone la necesidad revisión de reforzar la arquitectura regulatoria, mediante la identificación de divergencias legislativas significativas, lagunas jurídicas y limitaciones en los mecanismos de supervisión.

Abstract: Money laundering is a dynamic phenomenon that evolves in parallel with transformations in the international economic environment. Methods of illicit money laundering pose new challenges to authorities and financial institutions, largely driven by ongoing technological advancements. The use of emerging technologies gives rise to a layer of pseudonymity, which is no longer merely a technical feature; rather, it has evolved into a strategic instrument for criminal organisations seeking to sophisticate their laundering schemes by obscuring transactional traceability and the underlying economic and legal harms. This article analyses the problem of laundering illicit funds through crypto-assets by such organisations, as well as the various techniques employed to conceal traceability and identity. It first provides an in-depth examination of key international instruments, including the United Nations Convention against Transnational Organized Crime and the recommendations of the Financial Action Task Force (FATF), in relation to systems aimed at the prevention and suppression of illicit financial flows through crypto-assets. Building on this framework, this study undertakes a comparative analysis of the legislative approaches—markedly divergent—adopted in the United States and the European Union. This analysis goes beyond the mere identification of the problem; rather, it underscores the urgent need to strengthen regulatory frameworks by identifying significant legislative divergences, legal gaps, and the structural limitations of supervisory mechanisms.

Palabras clave: Criptoactivos, blanqueo de capitales, criminalidad organizada, seudonimidad digital, regulación financiera, tecnologías emergentes, darknet, transparencia y titularidad real.

Keywords: Crypto-assets, money laundering, organized crime, digital pseudonymity, financial regulation, emerging technologies, darknet, transparency, and beneficial ownership.

ABREVIATURAS

AML: *Anti-Money Laundering*. En español: lucha contra el blanqueo de capitales.

AMLA: *Anti-Money Laundering Authority*. En español, Autoridad Europea de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo.

AMLC: *Anti-Money Laundering Council*. En español: Consejo contra el blanqueo de capitales o dinero.

BARIS: *Bank Account Registers Interconnection System.* En español, Sistema de Interconexión de Registros de Cuentas Bancarias de la Unión Europea.

BC: Blanqueo de capitales.

BSA: *Bank Secrecy Act.* En español: Ley de Secreto Bancario.

CDD: *Customer Due Dilligence*. En español: Diligencia Debida en relación con el Cliente (DDC).

CEO: *Chief Executive Officer*. En español: director ejecutivo o Consejero Delegado, según el país.

CFT: *Countering the Financing of Terrorism*. En español: Lucha contra la Financiación del Terrorismo.

CFTC: *Commodity Futures Trading Commission*. En español: La Agencia Federal Independiente de Estados Unidos que regula los Mercados de Derivados (futuros, *swaps* y ciertas opciones).

DAO: *Decentralized Autonomous Organization*. En español: en el contexto del blanqueo de capitales (AML/CFT), es una organización nativa de *blockchain* que coordina decisiones y gestiona activos mediante *smart contracts* y gobernanza por tokens, sin una dirección central tradicional.

DEA: *Drug Enforcement Administration*. En español: Administración para el Control de Drogas.

EE. UU: Estados Unidos.

EUR: Moneda euro.

FATF: *Financial Action Task Force*. En español: GAFI.

FBI: *Federal Bureau of Investigation*. En español: Es la Agencia Federal de Inteligencia y Seguridad Interior de los Estados Unidos y su principal cuerpo policial federal.

FinCEN: *Financial Crimes Enforcement Network*. En español, suele traducirse como Red de Control/Ejecución de Delitos Financieros.

FT: Financiación del terrorismo.

GAFI: Grupo de Acción Financiera Internacional.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

IA: Inteligencia artificial.

IEEPA: *International Emergency Economic Powers Act.*, En español: Ley de Poderes Económicos en Emergencias Internacionales.

ICO: *Initial Coin Offering*. En español: Oferta Inicial de Monedas.

IRS: *Internal Revenue Service*. En español, la Agencia Federal de Recaudación de Impuestos de Estados Unidos.

KYC: *Know Your Customer*. En español: Conoce a Tu Cliente.

MiCA: *Markets in Crypto-Assets*. En español: Reglamento de Mercado de Criptoactivos.

NCA: *National Crime Agency*. En español: Agencia Nacional del Crimen del Reino Unido.

NYDFS: *New York State Department of Financial Services.* En español: Departamento de Servicios Financieros del Estado de Nueva York.

OC: Organización criminal.

PBC/FT: Prevención del blanqueo de capitales y financiación del terrorismo.

SEC: *Securities and Exchange Commission*. En español: Comisión de Bolsa y Valores de Estados Unidos.

SEPBLAC: Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

STR: *Suspicious Transaction Report*. En español: Reporte de Transacción Sospechosa.

UIF: Unidad de Inteligencia Financiera. Es el SEPBLAC en España (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias).

UNODC: *United Nations Office on Drugs and Crime.* En español: Oficina de las Naciones Unidas contra la Droga y el Delito.

UNTOC: *United Nations Convention against Transnational Organized Crime*. En español: Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

USD: *United States Dollar*, o dólar estadounidense.

VASP: *Virtual Asset Service Provider*. En español: Proveedores de Servicios de Activos Virtuales o CASP en el marco europeo.

6AMLD: Sexta Directiva para la Lucha del Blanqueo de Capitales y Financiación del Terrorismo.

1. INTRODUCCIÓN

En los últimos años, los criptoactivos han revolucionado el mundo de las finanzas, abriendo puertas para la innovación y la inclusión financiera como nunca se había visto. Pero este progreso tecnológico además ha abierto la puerta a nuevos desafíos, especialmente en el campo de la delincuencia financiera. Uno de los temas más preocupantes es el uso de los criptoactivos para el blanqueo de capitales (BC) por parte de las organizaciones o grupos criminales (OC).

Dichos activos generalmente operan en redes descentralizadas llamadas cadenas de bloques o (*blockchain*), que aseguran transacciones transparentes y seguras sin necesidad de un tercero centralizado como un banco (Bhutta et al., 2021). Al mover una criptomoneda, la transacción se registra en *blockchain*, que funciona como un libro de contable público distribuido por muchos ordenadores en el mundo. (Soltani et al., 2022) Las transacciones son verificadas por una red de usuarios conocidos como mineros, que son recompensados con nuevas unidades de criptoactivos (Binance Academy, 2024).

Durante décadas, el blanqueo de capitales (BC) ha sido una problemática a nivel internacional. La ocultación de la procedencia del fondo obtenido ilegalmente ha sido el objetivo principal de las OC con el firme propósito de darle una apariencia legal en los sistemas económicos. Las OC podían invertir con esta técnica sus ganancias ilegales sin dejar trazabilidad financiera que pueda llevar a su descubrimiento y procesamiento.

Las OC convencionales están altamente estructuradas con jerarquías y roles definidos para sus integrantes; (Enríquez Pérez, 2020) a menudo son apoyadas por políticos locales y emplean la corrupción para impedir problemáticas con la policía (Luna Galván et al., 2021). Operan mediante estructuras descentralizadas que dificultan la identificación de sus actividades. (UNODC, 2024). La estructura de dichas OC está diseñada para protegerlos de las fuerzas del orden y reducir el riesgo de infiltración o traición (UNODC.1, 2024). Para asegurar una definición común de la delincuencia organizada entre los Estados miembros, se creó la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La presente Convención establece la definición de una OC como un grupo estructurado de tres o más personas que actúan conjuntamente para cometer delitos con el objetivo de obtener un beneficio financiero directo o indirecto (Akkoyun & Çelik, 2022).

Las OC, con un alto nivel de especialización en el uso herramientas financieras complejas, cada vez más emplean las monedas virtuales para enmascarar el origen de su fondo ilícito (Trozze et al., 2022). Las OC emplean técnicas como el *layering*[1], los servicios de mezcla y las transferencias transfronterizas para dificultar la trazabilidad de los fondos. (Arnone et al., 2025). La incorporación de herramientas de análisis *blockchain* y el refuerzo de las obligaciones KYC/ PBC/FT (Prevención del blanqueo de capitales y financiación del terrorismo) posibiliten optimizar la detección y control de operaciones ilícitas. (Rodríguez-Valencia et al., 2025).

[1] El *layering* (o estratificación) es la segunda fase del proceso de blanqueo de capitales, en la que el objetivo principal es ocultar el origen ilícito de los fondos mediante una serie de transacciones financieras complejas, sucesivas y frecuentemente transfronterizas. Esta etapa busca romper la trazabilidad del dinero y dificultar que las autoridades puedan reconstruir el recorrido original de los fondos.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

El siguiente artículo aborda la problemática del blanqueo de fondos ilícitos a través de criptoactivos por parte de las OC y el marco jurídico existente para combatirlo. El análisis incluye las recomendaciones del GAFI, los instrumentos internacionales y las normativas de Estados Unidos (EE. UU) y la Unión Europea (EU) para prevenir el blanqueo con criptoactivos por parte de las OC. El presente trabajo examina, los tratados internacionales y las leyes nacionales de EE. UU y Europa que intentan prevenir el blanqueo por parte de las OC.

A partir de esta premisa, desarrollamos con el presente artículo, un análisis comparado de los modelos regulatorios de EE. UU y la EU, con el objetivo de identificar sus fortalezas y debilidades y formular criterios jurídicos de evaluación. Igualmente, el presente trabajo sostiene la eficacia del esfuerzo institucional para la mitigación contra el BC mediante criptoactivos, al no depender únicamente del desarrollo formal de los marcos normativos. Asimismo, su grado eficacia depende de la capacidad real para prevenir, detectar, atribuir y sancionar conductas ilícitas en un entorno caracterizado por la seudonimidad, la descentralización tecnológica y la dimensión transnacional del fenómeno.

La principal aportación radica en identificar la existencia de una brecha estructural entre la trazabilidad técnica de las transacciones en *blockchain* y su efectiva atribución jurídica, es la principal aportación de este estudio. Consecuentemente, los modelos convencionales de prevención, detección y sanción, incorporando capacidades tecnológicas en los sistemas regulatorios deben ser nuevamente replanteados.

2. METODOLOGÍA DE INVESTIGACIÓN

El presente documento utiliza un enfoque analítico descriptivo. El análisis será multidimensional, abordando la normativa, la literatura y la información para valorar las medidas de prevención del blanqueo de criptoactivos por parte de las OC. La revisión exploratoria de la literatura ya existente (libros, revistas, artículos, etc.) dará una mejor comprensión del concepto, la forma y las excelentes maneras de resolver esta problemática.

Este enfoque constituye la metodología más adecuada para desarrollar la investigación por déficit de información y por no existir artículos que hablen escasamente sobre las recomendaciones del GAFI, las convenciones internacionales y las leyes nacionales de EE. UU, Europa sobre la problemática del blanqueo con criptoactivos por parte de las OC.

Asimismo, el trabajo incorpora una dimensión analítica de carácter propositivo, orientada a identificar las limitaciones estructurales del marco jurídico actual en entornos digitales descentralizados.

3. ANÁLISIS DEL USO (INDEBIDO) DE LOS CRIPTOACTIVOS POR PARTE DE LAS ORGANIZACIONES CRIMINALES

La proliferación de servicios bancarios clandestinos y otras redes de blanqueo en línea ha generado canales de transferencia financiera más anónimos (Europol, 2022). Los criptoactivos tienen un potencial de un mal uso por parte de delincuentes, como resultado

de ello la industria está desarrollando nuevas formas complejas y servicios entre pares de mezcla. Ello genera las condiciones para ocultar las transacciones, el análisis regular descentralizado de *blockchain*, y las nuevas redes entre pares que recientemente han emergido para ser probablemente utilizadas en las actividades ilegales (Hinojal, 2023). Dichos desarrollos limitarán significativamente identificar actividades de las OC que utilizan las criptos convencionales para encubrir ganancias ilícitas (Fu et al., 2025).

El narcotráfico, el tráfico de armas y otras mercancías ilegales es un caso rentable, en la medida en que pueden mover fácilmente los fondos ilícitos hacia y desde OC en cualquier parte del mundo (Sudan et al., 2023). En efecto, más allá de las estafas, los criptoactivos han sido relacionadas con casi todos los tipos de delitos cibernéticos, desde los servicios en la *deep web*[2] o *darknet*[3] hasta el robo y el fraude en sus muchas formas.

Los criptoactivos han sido utilizados en una variedad de actividades de las OC, incluyendo el blanqueo, ataques *ransomware*[4] y fraude en línea. Con el fin de combatir estas prácticas ilícitas, se ha proporcionado a las fuerzas del orden una visión general de la literatura existente sobre el tema (Trozze et al., 2022). La investigación sobre el mal uso por parte de las OC aún es escasa en comparación con otros temas de investigación sobre criptoactivos y *blockchain*. Entre las actividades ilegales que realizan las OC con monedas digitales están el blanqueo (producto de delitos), el *ransomware* y los mercados negros (Alessi Longa, 2025).

Se han identificado siete categorías, cada una de las cuales condensa un patrón específico de comportamiento delictivo en la utilización de los criptoactivos y sus implicaciones para los mecanismos de prevención, detección y respuesta:

(1) La financiación del terrorismo, (2) en el BC, (3) en los mercados de la *deep web* o *darknet*, (4) en la ciberdelincuencia, (5) en el narcotráfico, (6) en la trata de personas, (7) y en la corrupción.

Centraremos nuestra investigación en la opción 2:

4. CRIPTOACTIVOS Y BLANQUEO DE CAPITALES POR PARTE DE LAS OC

Los criptoactivos recibidos por direcciones ilícitas en 2023 ascendieron a 46.100 millones de dólares estadounidenses (Chainalysis, 2025). En 2024 se desplomó el valor recibido por direcciones ilícitas hasta los 40.900 millones de dólares. Pero las cifras de 2024 son provisionales y podrían superar fácilmente los 51.000 millones de dólares (Atlam et al., 2024).

---

[2] La deep web (o web profunda) es la parte de Internet que no está indexada por los motores de búsqueda convencionales, como Google, Bing o Yahoo. Esto significa que su contenido no puede ser encontrado mediante búsquedas normales y solo es accesible si se conoce directamente la dirección, si se tiene autorización o si se utilizan credenciales específicas.

[3] La darknet es una parte específica y deliberadamente oculta de Internet que solo puede accederse mediante software, configuraciones o protocolos especiales que proporcionan anonimato, como Tor, I2P o Freenet. No está indexada por buscadores convencionales y está diseñada para proteger la identidad y ubicación de los usuarios y servidores.

[4] El *ransomware* es un tipo de software malicioso (*malware*) diseñado para bloquear, cifrar o inutilizar los sistemas informáticos de una víctima, con el objetivo de exigir un rescate económico —generalmente en criptomonedas— a cambio de la recuperación del acceso a los datos o sistemas.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Si bien algunos afirman que los criptoactivos tienen altos costos de información y control, en general las transacciones son más baratas y rápidas que las transacciones en monedas fiduciarias, puesto que no hay intermediarios entre compradores y vendedores (Medranda Morales & Arcos Argudo, 2023). Pero estas mismas características han sido aprovechadas por las OC para el blanqueo. En particular, tres características de los criptoactivos disminuyen drásticamente los costos de transacción de estas actividades ilegales.

En primer lugar, la naturaleza descentralizada de los criptoactivos posibilita a los usuarios intercambiar valor directamente entre ellos sin necesidad de intermediarios. Como ya se ha dicho, las normas tradicionales con el fin de combatir el blanqueo se dirigen a regular a los intermediarios que realizan operaciones para prevenir transferencias ilegales (Longa, 2025) y la ausencia de interacciones cara a cara en las transacciones con criptoactivos hace que sea más dificultoso la identificación de las partes intervinientes (Montoya Arrubla, 2025). En segundo lugar, si bien todas las transacciones quedan registradas y son rastreables en la *blockchain*, debido a que no hay una conexión explícita con individuos u organizaciones reales detrás de ellas. Los criptoactivos funcionan en un sistema seudónimo en el que solo se conoce la clave pública (una cadena aleatoria de números), pero la clave privada se mantiene en secreto.

Esto dificulta significativamente la vinculación de una identidad real a una dirección de criptomoneda (Béres et al., 2021). No obstante, los usuarios pueden generar múltiples carteras de criptoactivos electrónicos con diferentes direcciones públicas, lo que dificulta la rastreabilidad en caso de sospecha de blanqueo (Atlam et al., 2024).

Finalmente, la rapidez de las transacciones en criptoactivos y su facilidad de uso dan una ventaja sobre los métodos tradicionales de blanqueo, como el efectivo. A diferencia del dinero en papel, que está limitado por el peso y el tamaño, los criptoactivos se pueden almacenar en cantidades ilimitadas en una memoria USB y enviarse a cualquier persona en el mundo en cuestión de minutos. La maleabilidad de las transacciones facilita eludir las medidas regulatorias, al poder fraccionar una transacción grande en otras más pequeñas (Koelbing et al., 2024). Esta flexibilidad operativa es vital y refuerza el BC para las OC que operan en los mercados de criptoactivos. Dichos equipos generan un gran volumen de criptoactivos, que necesitan transformar en fondos con apariencia legal.

Este proceso generalmente involucra una serie de transacciones financieras complejas que mueven los fondos a través de múltiples cuentas y jurisdicciones, haciendo arduo rastrear el origen de los fondos. Lo que posibilita a las OC seguir operando en la ilegalidad y ocultar las ganancias del narcotráfico (FATF, 2022). Las OC que utilizan la *deep web*, son maestras en el blanqueo de criptoactivos, las cuales pueden ser transferidas instantáneamente de una cuenta a otra y son dificultosos de rastrear (Holt et al., 2023). Dichas OC a menudo contratan facilitadores profesionales (abogados, contadores, banqueros, etc.) para dificultar la trazabilidad de sus fondos ilícitos.

Las OC pueden retener como inversión los criptoactivos que reciben en las operaciones del mercado cripto. Se emplean para blanquear otras monedas ilícitas en línea y en el mundo real (Arnone et al., 2025). Las que no se mantienen como inversión se blanquean e introducen en la economía legal. Por ejemplo, la policía holandesa descubrió

que un moderador de un mercado cripto aprovechaba sus contactos para canjear bitcoins por efectivo (Ministerio del Interior, 2024).

En Asia oriental y sudoriental, las organizaciones «*point runners*» o «*moving ants*» son utilizadas para blanquear fondos ilícitos, reclutando a muchas personas (a menudo jóvenes desempleadas) que prestan sus cuentas bancarias y generan empresas ficticias para ocultar la fuente y el destino del fondo ilícito (UNODC, 2025). Estas redes mueven el fondo a través de múltiples cuentas bancarias o de criptoactivos y casinos en línea, donde se disfraza como ganancias legítimas de casino (Langdale, 2024).

Ahora que las autoridades conocen mejor los pagos de terceros (tras la «*Operación Chain Break*» y otras similares en China) (FinCEN, 2025), los OC han recurrido cada vez más a los criptoactivos para sus operaciones de juego ilegal, lo que plantea serios desafíos para los investigadores (Europol, 2024). Por ejemplo, los casinos y operadores de *junkets*[5] con licencia en Filipinas estuvieron involucrados en el blanqueo de unos 81 millones de dólares sustraídos en un ciberataque de 2016 atribuido al grupo Lazarus del Banco Central de Bangladesh (Langdale, 2024). Aunque el fondo pasó por bancos y empresas de envío de remesas, fue extremadamente complejo rastrearlo una vez que llegó a las manos de los operadores de viajes de juego del casino (AMLC, 2023).

Los cárteles mundiales de la droga fueron acusados por la DEA de utilizar *Binance,*[6] por ser el mayor cripto intercambiador al blanquear en diversas transacciones entre 15 y 40 millones de dólares (DEA, 2025). De conformidad con los informes de la DEA, *Binance* está colaborando con los investigadores en medio del escrutinio por diversas denuncias.

Dichos sofisticados mecanismos, generan nuevos desafíos para ser detectados e investigados por el número de transacciones y su naturaleza transfronteriza, exigiendo mayor transparencia financiera, cooperación internacional y marcos regulatorios más sólidos para combatir dichos delitos (Legrand & Leuprecht, 2021).

5. MÉTODOS MÁS COMUNES DE BLANQUEO DE CRIPTOACTIVOS UTILIZADO POR LAS OC

5.1. CONSIDERACIONES GENERALES DESDE LA DOGMÁTICA DEL BLANQUEO DE CAPITALES

El fenómeno conceptualizado pone de manifiesto que las distintas técnicas empleadas por las OC se insertan dentro de las fases clásicas del BC, en particular la colocación, la estratificación y la integración.

Estas prácticas descritas en el apartado anterior son las que generan las problemáticas en relación con la tipicidad, atribución de responsabilidad y reconstrucción

[5] Los operadores de junkets son intermediarios especializados que actúan entre los casinos y los jugadores VIP o high-rollers, especialmente en mercados como Macao, Las Vegas, Singapur y otros centros internacionales de juego. Su función principal es reclutar, transportar, financiar y gestionar a clientes de alto valor para que jueguen en determinados casinos.

[6] Binance es el mayor exchange de criptomonedas del mundo por volumen de negociación y número de usuarios, fundado en 2017 por Changpeng Zhao (CZ) y Yi He. Es una plataforma centralizada (CEX) que permite comprar, vender, intercambiar y custodiar activos digitales.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

del itinerario financiero de los fondos ilícitos. Especialmente, en un entorno caracterizado por la seudonimidad y la descentralización tecnológica como son los criptoactivos.

5.2. TÉCNICAS VINCULADAS A LA FASE DE INTEGRACIÓN: EL *SMURFING*

La práctica conocida como *smurfing*, pitufeo o menudeo implica la integración en el sistema financiero, de forma variada y de poca cantidad, de fondos obtenidos por actividades ilícitas, monedas procedentes del narcotráfico, pagos por fraude, corrupción o ganancias originarias de la explotación sexual (Isolauri & Ameer, 2023). Esta técnica, utilizada en las finanzas convencionales, parece haberse trasladado al mundo de los criptoactivos (Koelbing et al., 2024).

Desde el punto de vista jurídico penal, esta clase de prácticas pueden encajar en la fase de integración del BC. Dejamos claro, la intención de introducir fondos ilícitos en el sistema financiero oficial, mediante su fraccionamiento, para eludir los mecanismos de control. Desde una perspectiva jurídica, plantea cuestiones relevantes acerca de la aplicación de umbrales regulatorios y la eficacia de los sistemas de detección automatizada.

5.3. TÉCNICAS VINCULADAS A LA FASE DE ESTRATIFICACIÓN: OCULTACIÓN Y DISOCIACIÓN DEL ORIGEN ILÍCITO

5.3.1. Cartera de criptoactivos (monederos medianos) (medium wallets o mid-size wallets)

Un método usual de BC con criptoactivos implica el uso de carteras intermediarias. Esta técnica de estratificación busca disimular la vinculación entre los fondos ilícitos y su posterior entrada al sistema financiero legal. (Elliptic, 2024). En consecuencia, las carteras intermediarias están siendo utilizadas por los delincuentes en los *exchange* con y sin KYC.

Desde el punto de vista dogmático, las cuentas interpuestas y su utilización está directamente vinculada a la fase de estratificación del BC, al ser destinadas a dificultar la trazabilidad de los fondos ilícitos. Se generan retos esenciales respecto de la atribución objetiva y la identificación del titular económico, con estas conductas descritas, en particular cuando no hay puntos de contacto con intermediarios obligados a identificar.

5.3.2. Carteras de criptoactivos de consolidación

Las carteras de consolidación, que agrupan y combinan fondos de diversas fuentes, son otra tendencia a tener en cuenta. Este patrón de consolidación puede poner de manifiesto los intentos de ocultar el origen ilícito de los fondos antes de moverlos a bolsas u otros lugares de retiro de efectivo (Chiang, 2024).

Estas estructuras, desde un punto de vista jurídico podrían ser consideradas como instrumentos diseñados para reforzar la ocultación del origen ilícito de los fondos. Esta circunstancia afecta de manera directa en la configuración típica del delito de BC en su modalidad de ocultación o encubrimiento.

5.3.3. Servicios de mezcla, monedas de privacidad y puentes

El objetivo de la mezcla y el barajado, es separar las elevadas cantidades de monedas virtuales, distribuyéndolas en múltiples direcciones (Gorjón, 2023). Los mezcladores son individuos o empresas que distribuyen los fondos entre los participantes y los mezclan con ingresos lícitos con el fin de ocultar la trazabilidad e identificación de los propietarios (Coinmetro Editorial Team, 2024).

Las problemáticas específicas de tipicidad en la fase de ocultación del BC que plantea el uso de servicios de mezcla, están diseñados precisamente para dificultar la trazabilidad de los fondos. Consecuentemente, esta problemática cuestiona el alcance de las obligaciones de diligencia debida de los proveedores de servicios de activos virtuales (VASP) o CASP. en el marco europeo. La referida circunstancia viene prevista en el artículo 13 de la Directiva (UE) 2015/849, especialmente cuando dichos operan en jurisdicciones con supervisión limitada o inexistente.

Las monedas de privacidad intensifican las problemáticas asociadas a la atribución de las transacciones, al reforzar la seudonimidad en el plano identitario. Dicho genera una esencial limitación operativa probatoria en el proceso penal, en particular en lo relativo a la vinculación entre direcciones y personas físicas o jurídicas concretas. Las monedas de privacidad se han vuelto populares para quien quiere pasar desapercibido. (Cremers et al., 2024).

La transferencia de activos entre diferentes *blockchain* es una técnica conocida como puentes criptográficos, siendo el método o herramienta cada vez más popular para el BC.

El uso de puentes entre *blockchain* desde un punto de vista jurídico, agrava la dimensión transnacional del BC, al generar problemáticas de competencia jurisdiccional y cooperación internacional, así como limitación operativa adicional en la reconstrucción del itinerario financiero de los fondos.

5.4. ESPACIOS CRIMINÓGENOS Y FACILITADORES: MERCADOS DE LA *DARKNET*

Los mercados de la *darknet* son sitios ocultos en línea a los que se accede mediante software específico (como Tor) y se paga en criptoactivos anónimos. Dichos mercados facilitan el comercio de bienes y servicios ilegales y dan a los blanqueadores una forma de convertir los fondos ilícitos en criptoactivos y viceversa (Jordá et al., 2024). Es extremadamente complejo saber con precisión cuántos fondos ilícitos se blanquea con este activo virtual (Alessi Longa, 2025).

En la darknet, *Silk Road* fue el mercado más popular que funcionaba en la red *Tor,* debido a que posibilitaba la comercialización anónima con criptoactivos. A pesar de intentar mantenerse en la seudonimidad, fue detenido su fundador Ulbricht por el FBI en 2013 y finalmente condenado por varios cargos.

En vista de la gran cantidad de blanqueadas, resulta pertinente examinar el marco jurídico existente con el fin de combatir el blanqueo de criptoactivos por parte de los OC. Dichos entornos refuerzan los desafíos estructurales de intervención de las autoridades y

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

plantean desafíos regulatorios y operativos tanto en la obtención de prueba digital como en la identificación de los sujetos intervinientes, lo que incide directamente en la eficacia de la persecución penal del BC. El caso ilustró los desafíos de regular y monitorear la *deep web* (Hemdani, 2025).

5.5. CONSIDERACIÓN DOGMÁTICA FINAL

Todas estas técnicas ponen de manifiesto los límites del Derecho penal convencional para adaptarse a estructuras tecnológicas descentralizadas. Esto plantea interrogantes sobre la delimitación de la tipicidad y la eficacia de las respuestas normativas en un entorno digital en constante evolución.

6. MARCOS JURÍDICOS PARA COMBATIR EL BLANQUEO DE CRIPTOACTIVOS POR PARTE DE LAS OC

Los marcos legales para los criptoactivos están altamente fragmentados a nivel mundial, con algunos países prohibiéndolas por completo y otros abrazándolas por completo. Se ha intentado por medio de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) para combatir la delincuencia organizada transnacional.

6.1. CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA DELINCUENCIA ORGANIZADA TRANSNACIONAL

La Convención de la UNTOC, de 2000, es el principal instrumento jurídico internacional para hacer frente a los desafíos de la delincuencia organizada transnacional. Ofrece un conjunto de instrumentos para que los Estados desarrollen políticas y marcos legales para prevenir y combatir las diferentes formas de delincuencia organizada, como el BC asociado a los criptoactivos (Kabra & Gori, 2025). Esta convención es relevante, en la medida en que dichos activos virtuales están tomando un papel más grande en el mundo financiero de las OC. La UNTOC puede apoyar la persecución y prevención contra el blanqueo de criptoactivos mediante el desarrollo de marcos legales más fuertes, la cooperación internacional y la aplicación de estándares comunes para combatir las transacciones ilegales de este activo virtual (Wang & Hsieh, 2023).

En sus artículos 1, 13, 16 y 18 se regula la cooperación transfronteriza para la asistencia jurídica mutua, la extradición y el intercambio de información. Como las transacciones con criptoactivos pueden involucrar a varias jurisdicciones, la atención de la UNTOC en la cooperación internacional es esencial para encontrar y llevar ante la justicia a los OC que abusan de este activo virtual. Por ejemplo, la Agencia Nacional contra el Crimen (NCA) del Reino Unido desmanteló una red masiva de BC de miles de millones de dólares llamada Operación Desestabilizar (Anggriawan & Susila, 2024).

Esta red atendía a una amplia gama de OC, desde rusos ricos y personas influyentes globales hasta ciberdelincuentes y narcotraficantes. La NCA identificó a dos OC de habla rusa, «*Smart*» y «*TGR*», como los autores intelectuales. Hasta el momento su investigación ha llevado a 84 detenciones y la incautación de más de 20 millones de euros en efectivo y en criptoactivos (UNODC2, 2024). Esta operación exitosa fue posible gracias al trabajo conjunto de los firmantes de la convención, entre los que se encuentran

el Servicio de Policía Metropolitana del Reino Unido, la *Direction Centrale de la Police Judiciaire* de Francia, la Oficina de Control de Activos Extranjeros del Tesoro de Estados Unidos, la Agencia Antidrogas y el FBI. (FATF et al., 2025).

El artículo 34 de la UNTOC alienta a los Estados a tomar medidas legislativas compatibles para prevenir el BC, lo que es fundamental para abordar los riesgos crecientes de delitos financieros relacionados con criptoactivos. Por ejemplo, el GAFI requiere medidas KYC y de debida diligencia del cliente para identificar e informar transacciones sospechosas de criptoactivos, las cuales deben ser implementadas en todos los países, independientemente de sus leyes locales. (FATF, 2024).

La UNTOC apoya el desarrollo de estándares internacionales, asistiendo a los países en el desarrollo de capacidades optimizadas de ciberseguridad e investigación para detectar delitos relacionados con criptoactivos. UNODC. (2026) Por ejemplo, los canales de intercambio de información de la UNTOC apoyan a las agencias policiales de la UE, como Europol, en el rastreo de transacciones ilegales en este activo virtual. Esto puede involucrar en este sentido a Eurojust, la agencia de la UE para la cooperación judicial, para asegurar una persecución transfronteriza efectiva.

En este contexto, la UNTOC ofrece un enfoque internacional con el objetivo de combatir el blanqueo de criptoactivos, al promover la cooperación internacional, la armonización jurídica y el desarrollo de capacidades en materia de aplicación de la normativa.

6.2. RECOMENDACIONES DEL GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL

El GAFI ha establecido un conjunto integral de estándares encaminados a mitigación y lucha del BC/FT que abarca los activos virtuales y los proveedores de servicios de activos virtuales (VASP). Desde una perspectiva jurídica, el GAFI define «activos virtuales» y «proveedores de servicios de activos virtuales» para garantizar la aplicación coherente y uniforme de sus estándares. Los activos virtuales son una representación digital de valor que se puede negociar o transferir digitalmente y que se puede utilizar para realizar pagos o inversiones (FATF, 2023).

Los VASP abarcan cualquier persona física o jurídica no cubierta en otro lugar por las Recomendaciones y que, como negocio, se dedique a una o más de las siguientes actividades: el intercambio entre activos virtuales y monedas fiduciarias; entre una o más formas de otros activos virtuales; la transferencia de activos virtuales; la custodia y/o administración de activos virtuales o instrumentos que permitan regular activos virtuales; y la participación y provisión de servicios financieros relacionados con la oferta y/o venta de un activo virtual por un emisor (FATF, 2021).

Desde una perspectiva jurídica, la Recomendación 15 trata específicamente de los activos virtuales, al disponer que, los países deben identificar y atenuar los riesgos de PBC/FT relacionados con activos virtuales y VASP. El GAFI requiere que se apliquen la debida diligencia del cliente (CDD), el mantenimiento de registros, la notificación de transacciones sospechosas (STR), los controles internos y los programas de cumplimiento, y las sanciones (FATF.1, 2023). Igualmente, la Recomendación 16 exige a los VASP obtener, conservar y transmitir la información del ordenante y del beneficiario

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

en las transferencias de activos virtuales por encima de un umbral determinado (1.000 USD/EUR). A veces se le llama «regla de viaje».[7]

Esta norma busca prevenir el uso de activos virtuales para fines ilegales y asegurar la transparencia en las transacciones, en la medida en que requiere a los VASP compartir esta información con otras entidades obligadas. La norma de viaje para activos virtuales ha sido una prioridad para el GAFI y continúa presionando a los países para que la implementen y hagan cumplir (Mollaahmetoğlu & Baykut, 2021).

El GAFI va actualizando sus recomendaciones sobre activos virtuales para estar al día con los riesgos cambiantes y las innovaciones tecnológicas en el mundo de los activos virtuales. Los países deberían de incorporar estas reglas en sus leyes y regulaciones nacionales. El GAFI continúa monitoreando la implementación de estas normas en todo el mundo e insta a las jurisdicciones a priorizar su implementación efectiva (Teng et al., 2026).

7. MODELOS NORMATIVOS TRANSATLÁNTICOS ANTE EL BLANQUEO DE CAPITALES CON CRIPTOACTIVOS: EVALUACIÓN COMPARADA EE. UU–UE

7.1. ESTADOS UNIDOS

En EE. UU no existe un marco regulatorio unificado para los criptoactivos; en cambio, varias agencias federales y estatales supervisan dichos activos virtuales. La *Securities and Exchange Commission*, o Comisión de Bolsa y Valores de EE. UU (SEC) controla los valores y ha considerado muchos criptoactivos y ofertas iniciales de monedas (ICO) como valores. En SEC v. *Decentralized Autonomous Organization* (DAO), sostuvo que los criptoactivos son valores y, por lo tanto, están sujetas a la regulación de la SEC (Lom & Hashmall, 2021). La *Commodity Futures Trading Commission*, o Agencia Federal Independiente de EE. UU que regula los Mercados de Derivados (CFTC) considera al bitcoin y otros activos virtuales como materias primas y regula los mercados de derivados y futuros sobre criptoactivos. (Hinojal, 2023).

El *Financial Crimes Enforcement Network*, o Red de Control/Ejecución de Delitos Financieros (FinCEN) controla los cripto intercambios y los proveedores de billeteras electrónicas como transmisores de fondos, y deben cumplir con las regulaciones PBC/FT y KYC. La *Internal Revenue Service*a (IRS), o Agencia Federal de Recaudación de Impuestos de Estados Unidos, trata a los criptoactivos como propiedad para fines fiscales, y las ganancias y pérdidas están sujetas al impuesto sobre las ganancias de capital (Baer et al., 2023). La regulación tiende a ser descentralizada; estados como Nueva York tienen

[7] La Regla de Viaje es una obligación establecida por el Grupo de Acción Financiera Internacional (GAFI/FATF) que exige a las entidades financieras y a los proveedores de servicios de activos virtuales (VASPs) transmitir información sobre el originador y el beneficiario junto con la transferencia de fondos o criptoactivos. Su finalidad es garantizar la trazabilidad y permitir a las autoridades identificar a las partes involucradas en transacciones que puedan estar vinculadas con blanqueo de capitales, financiación del terrorismo u otros delitos graves.

sus propias leyes (*BitLicense*),[8] mientras que otros tienen políticas más laxas o indefinidas.

La *BitLicense* es una licencia de negocios que requiere de los operadores unas reglas PBC/FT más estrictas. En California, la ley requiere que los operadores de bitcoins tengan reservas equivalentes a las de los bancos para cubrir pérdidas, pero Carolina del Norte aún está trabajando en los proyectos de ley de regulación de bitcoins y no tiene ninguna directiva vigente (NYDFS, 2024–2026).

La fiscalía general de los EE. UU abrió un caso penal contra *Rule y Nysewander*[9] por conspirar con otros para blanquear las ganancias ilícitas de estafas amorosas en línea, estafas de correo electrónico empresarial, estafas inmobiliarias y otros fraudes a través de criptoactivos (Lim & Choi, 2025).

De acuerdo con la acusación con la fiscalía general de los Estados Unidos, habían llevado a cabo la conversión el fondo ilícito en criptoactivos y lo transfirieron a cuentas controladas por sus cómplices en EE. UU y en el extranjero. Esto evidencia una estrategia destinada a ocultar el origen ilícito de los fondos y dificultar su trazabilidad. Así mismo, al abrir cuentas y operar con bancos y plataformas de *exchange* o cripto intercambios, *Rule y Nysewander* habrían realizado declaraciones falsas y omitida información relevante con el fin de evadir los controles y salvaguardias propios de estas instituciones.

Como resultado de estas actuaciones, en esta supuesta conspiración, ellos y sus cómplices blanquearon más de 2,4 millones de dólares estadounidenses. Finalmente, ambos fueron declarados culpables y podrían enfrentarse a cargos de hasta 20 años de prisión federal por cada cargo de BC (Farrukh et al., 2025).

Igualmente, en agosto de 2024, se imputó a Lam y Serrano por el robo de criptoactivos por 230 millones de dólares estadounidenses (Trozze et al., 2022).

Los fiscales estadounidenses también han ido tras *Binance*, la empresa que opera la mayor plataforma mundial de intercambio de criptoactivos, *Binance.com*. La empresa se ha declarado culpable y pagará más de 4.000 millones de dólares para resolver la investigación del Departamento de Justicia sobre violaciones de la Ley de Secreto Bancario (BSA), por no registrarse como transmisor de fondos, y de la Ley de Poderes Económicos de Emergencia Internacional (IEEPA) (U.S. Department of Justice, 2023).

El canadiense Changpeng Zhao, fundador y ex CEO de *Binance*, también se declaró culpable de no mantener un programa efectivo contra el BC (PBC/FT o AML), en violación de la ley BSA. Como parte del acuerdo de culpabilidad, Zhao ha renunciado como CEO de Binance (U.S. Department of Justice.1, 2023).

[8] La *BitLicense* es una licencia regulatoria obligatoria emitida por el New York State Department of Financial Services (NYDFS) para las empresas que realizan actividades con criptomonedas o activos virtuales en el estado de Nueva York o con residentes de Nueva York. Fue introducida en 2015 mediante el reglamento 23 NYCRR Part 200.

[9] Son dos hombres (de Nevada y Carolina del Sur) que fueron acusados y posteriormente condenados por participar en una conspiración de blanqueo mediante criptomonedas, según el Departamento de Justicia de EE. UU.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Si bien, los fiscales estadounidenses han logrado enjuiciar con éxito a los blanqueadores de capitales y a las plataformas *exchange* o de cripto intercambios, el mercado de los criptoactivos aún requiere mayores niveles de transparencia, a fin de proteger a los inversores potenciales (Anguren et al., 2023). Hace unas décadas el auge del comercio electrónico provocó marcos legales de carácter o naturaleza innovadora actual a dichos activos virtuales y sus muchas formas merecen una guía similar. La creación de reglas claras para la venta de ciertas criptomonedas y fondos cripto podría proporcionar la claridad que tanto se necesita (Blanco Barón, 2025).

Sin un marco regulatorio más maduro, depender solo de las acciones coercitivas de agencias como la SEC no resulta suficiente para alcanzar sus objetivos regulatorios. En última instancia, estas acciones punitivas pueden perjudicar a los mismos inversores que la SEC busca proteger y sofocar la inversión en empresas prometedoras. Entre la normativa planteada para los criptoactivos está el proyecto de ley contra el blanqueo de activos digitales, con la que se busca prevenir otros delitos relacionados con los activos virtuales, pero poniendo el foco en quienes realizan las transacciones (mineros, validadores, etc.) (Warren & Marshall, 2022).

El sistema norteamericano desde una perspectiva jurídica se caracteriza por ser segmentado y reactivo, puesto que intervienen múltiples agencias con competencias interrelacionadas. La flexibilidad regulatoria que brinda esta estructura puede generar problemáticas de coherencia normativa y posibles solapamientos competenciales.

Este enfoque tiene limitaciones en la prevención *ex ante* cuanto hablamos de BC, en la medida en que su actuación se centra básicamente en mecanismos de *enforcement* posteriores a la comisión del ilícito. El déficit normativo de un marco unificado, de igual modo impide la aplicación uniforme de las obligaciones de cumplimiento por parte de los proveedores de servicios de activos virtuales (VASP), en este contexto podría generar espacios de riesgo regulatorio.

7.2. UNIÓN EUROPEA

Hoy en día la UE no cuenta con un marco jurídico armonizado para los criptoactivos en todos los Estados miembros. Pero la Comisión Europea ha propuesto algunas medidas, como la Sexta Directiva contra el blanqueo de capitales (6AMLD), que exigiría a las empresas que trabajan con criptoactivos registrarse ante las autoridades nacionales.

Seguir las normas antiblanqueo de capitales e informar de cualquier transacción sospechosa. El objetivo de la 6AMLD es colmar las lagunas jurídicas de las leyes individuales de los países de la UE mediante la creación de definiciones coherentes para el BC y los activos virtuales en toda la UE (Parlamento Europeo, 2024).

Para establecer una manera uniforme de regular las negociaciones con criptoactivos en toda la EU, la Comisión Europea recomendó el Reglamento del Parlamento Europeo y del Consejo sobre los mercados de criptoactivos y la Directiva en modificación. Este

conjunto de normas, denominado MiCA,[10] tiene por objeto establecer una estructura de supervisión, que incluye normas para quienes los emiten, los proveedores de servicios y los participantes en el mercado secundario.

Utilizando estas regulaciones MiCA y 6AMLD, el 19 de septiembre de 2024, la Policía Criminal Federal Alemana desmanteló las infraestructuras de 47 plataformas de cripto intercambio en ruso sin verificación de identidad (sin protocolo KYC). Esta operación, denominada «Operación Final Exchange», es de gran envergadura y evidencia el papel crucial que tienen las plataformas de intercambio (*exchange*) instantáneo sin KYC en el cibercrimen (Menacho-Inga et al., 2025). Como sus nombres implican, dichos sitios sin protocolos de KYC no tienen ningún proceso visible para recopilar información de identificación de los usuarios antes de permitirles depositar o retirar cualquier cantidad. No piden nombres, números de teléfono ni correos electrónicos y no se molestan en verificar esta información antes de realizar las transacciones (Anggriawan & Susila, 2024).

Una de las mayores vulnerabilidades del marco normativo actual de los criptoactivos es la falta de una autoridad central con la capacidad de supervisar y auditar las transacciones. Asignar la supervisión y regulación de los criptoactivos a agencias no especializadas reduce el efecto de estas regulaciones. Asimismo, en el ámbito legal no existen lineamientos ni requisitos previos para adquirir licencias para operar en negocios de criptoactivos (Hope Kanu, 2025).

Desde una perspectiva comparada, el modelo estadounidense presenta un enfoque fragmentado y reactivo, basado en la actuación posterior de distintas agencias. Por otro lado, el modelo de la EU se caracteriza por un enfoque preventivo y armonizado, el cual está orientado a disminuir la seudonimidad *ex ante*. Sin embargo, ambos sistemas tienen en su capacidad operativa, las limitaciones para hacer frente al ámbito internacional del fenómeno.

No es plenamente eficaz ninguno de los dos sistemas. El modelo estadounidense en la fase preventiva puede tener lagunas, mientras que el modelo europeo en su aplicación efectiva y en adaptarse a la rápida evolución tecnológica del ecosistema cripto, sigue enfrentando desafíos.

8. NOVEDADES LEGISLATIVAS DE LA UNIÓN EUROPEA

Las estructuras societarias opacas empleadas por las OC para blanquear los activos virtuales, con entrada en vigor el 10 de julio de 2027 que, reforzará la transparencia de la titularidad real, amplía la trazabilidad y el control sobre las operaciones con criptoactivos, prohibiendo las cuentas anónimas (Rgto. (UE) 2024/1624 art.79.1) y exigirá medidas específicas para las transferencias a direcciones autohospedadas[11] (Rgto. (UE) 2024/1624 art.40).

[10] Son las siglas de *Markets in Crypto-Assets Regulation*, el Reglamento (UE) 2023/1114 sobre los mercados de criptoactivos. Es la primera norma integral de la EU que regula los criptoactivos, sus emisores y los proveedores de servicios vinculados a ellos.

[11] Una dirección autohospedada o autoalojadas es una dirección de criptomonedas controlada directamente por un usuario, sin intervención ni custodia de un intermediario regulado (como un exchange o un VASP).

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Al mismo tiempo, el paquete normativo anterior, ha sido remozado por una nueva Directiva sobre mecanismos de prevención, que introduce la obligación estatal de establecer mecanismos para identificar a la persona que posee o controla cuentas de criptoactivos y de interconectar dichos mecanismos a través de un sistema a nivel de la UE (Dir. (UE) 2024/1640 art.16). Desde una perspectiva jurídica, se refuerza la supervisión europea con la creación de la Autoridad AMLA, que es plenamente operativo desde el pasado 1 de julio de 2025 (Rgto. (UE) 2024/1620).

8.1. ¿QUÉ CAMBIOS INTRODUCE LA UE CON RESPECTO A LOS EE. UU PARA MITIGAR LA SEUDONIMIDAD Y LA OPACIDAD EN EL USO DE CRIPTOACTIVOS?

La UE prohíbe a los proveedores de servicios de criptoactivos mantener cuentas de anónimas o cualquier cuenta que permita ocultar al titular o aumentar el oscurecimiento de las transacciones, mencionándose específicamente las monedas de privacidad (Rgto. (UE) 2024/1624 art.79.1). En línea con ese enfoque, el paquete PBC/FT europeo establece la obligación a los proveedores de servicios de criptoactivos que identifiquen y evalúen riesgos inherentes en transferencias con direcciones autoalojadas. Igualmente, dichos proveedores deben y aplicar medidas de mitigación proporcionales, que pueden llegar a incluir la identificación y verificación del remitente o del receptor y la recopilación de información adicional sobre el origen y el destino (Rgto. (UE) 2024/1624 art.40.1). Estas normas consolidan el objetivo de limitar el uso de criptoactivos para fines de anonimización, en particular cuando se combinan con estructuras societarias opacas, el contexto que el propio marco europeo reconoce que genera riesgos de elusión y ofuscación y al que da respuesta el nuevo paquete de 2024.

La UE ha preferido adoptar el modelo de «tolerancia cero» a la seudonimidad, con prohibiciones directas, reglas uniformes y una nueva autoridad supranacional. En cambio, EE. UU sigue un modelo descentralizado donde el anonimato no está prohibido, y las autoridades actúan principalmente a través de acciones penales o administrativas tras detectar infracciones.

La gran diferencia es simple. La UE limita la seudonimidad *ex ante* mediante prohibiciones y EE. UU lo combate *ex post* mediante *enforcement.*[12]

[12] Es un término anglosajón que se traduce como aplicación, ejecución o hacer cumplir la ley. En el ámbito jurídico y regulatorio describe el conjunto de acciones, medidas y procedimientos que llevan a cabo las autoridades competentes para garantizar que las normas se cumplan efectivamente. En términos generales: *Enforcement* es la capacidad y práctica de un Estado o autoridad reguladora para investigar, supervisar, sancionar y corregir incumplimientos normativos.

Tabla 1.
Diferencias clave UE vs. EE. UU en seudonimidad y opacidad en criptoactivos.

DIMENSIÓN	UE	EE. UU
Cuentas anónimas.	Prohibidas explícitamente (art. 79.1).	No prohibidas por ley federal.
Monedas de privacidad	Prohibición a partir de 2027.	No prohibidas, pero vigiladas.
Cartera de criptoactivos autoalojadas.	Evaluación obligatoria de riesgos e identificación posible. (art. 40.1).	No existe obligación federal de identificación.
Marco regulatorio.	Integral, unificado (MiCA + AMLR).	Fragmentado: SEC, CFTC, FinCEN, IRS, estados.
Supervisión.	Centralizada bajo AMLA.	Descentralizada; cada agencia actúa en su ámbito.
Tokens privados.	Eliminación total.	No prohibidos.
Enfoque.	Preventivo, restrictivo, trazabilidad total.	Reactivo, sancionador, basado en *enforcement*.

8.2. ¿QUÉ NOVEDADES AFECTAN A LA IDENTIFICACIÓN DEL TITULAR REAL Y A LA TRANSPARENCIA SOCIETARIA FRENTE A ESTRUCTURAS OPACAS?

El Reglamento (UE) 2024/1624 especifica la cadena de identificación del titular real por propiedad y control, y que la información de titularidad real sea adecuada, precisa y actualizada, y que las entidades informen al registro central sin dilación indebida y dentro de un plazo máximo de 28 días naturales para comunicar cualquier cambio (Rgto. (UE) 2024/1624 art.63). La información para obtener datos del titular real se amplía y específica, incluyendo, entre otras, la identificación completa, la naturaleza y extensión del interés real y, en caso de existir una estructura con múltiples entidades o instrumentos, la descripción de la estructura de propiedad y control (Rgto. (UE) 2024/1624 art.62). Desde una perspectiva jurídica, la Directiva (UE) 2024/1640 establece normas sobre el establecimiento y el acceso a registros centrales de titularidad real y sustituye a la Directiva (UE) 2015/849, que queda derogada a partir del 10-7-2027 (Dir. (UE) 2024/1640; efecto derogatorio).

Todo ello en línea con el refuerzo del marco de transparencia y cooperación en toda la UE con el objetivo de limitar significativamente el recurso a empresas pantalla o entramados societarios opacos.

Por el contrario, Estados Unidos, facilita el recurso de entramados societarios, al dar un giro de 180º, mitigando drásticamente la transparencia, al eliminar las obligaciones para las empresas estadounidenses, debilitando el *Corporate Transparency Act*[13] y dejando la transparencia en manos de los estados.

[13] El *Corporate Transparency Act* (CTA) es una ley federal de Estados Unidos, promulgada en 2021, cuyo objetivo es combatir el blanqueo de capitales, la financiación del terrorismo, el fraude fiscal y el uso de sociedades pantalla mediante la obligación de reportar información sobre los beneficiarios reales (*Beneficial Ownership Information*, BOI) de determinadas entidades.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Tabla 2.
Comparación del marco de transparencia de la titularidad real y supervisión PBC/FT: Unión Europea vs. Estados Unidos.

ELEMENTO	UNIÓN EUROPEA	ESTADOS UNIDOS
Cadena de identificación del titular real.	Detallada, ampliada y obligatoria (propiedad + control, extensión del interés, estructura societaria completa).	Eliminada casi por completo para entidades nacionales desde 2025; solo aplica a algunas entidades extranjeras.[14]
Actualización de datos.	Máximo 28 días naturales para notificar cambios.	No existe obligación federal para empresas estadounidenses.
Registros centrales.	Obligatoriedad y armonización bajo Dir. 2024/1640.	No hay registro federal para entidades domésticas tras la IFR de 2025; transparencia depende de los estados. [15]
Estrategia frente a empresas pantalla.	Restrictiva, preventiva y basada en trazabilidad integral.	Relajación normativa: desaparición del sistema de reporte federal facilita el uso de estructuras societarias opacas.
Supervisión AML PBC/FT.	Modelo europeo unificado con AMLA.	*Enforcement* fragmentado (FinCEN, IRS, SEC, CFTC), sin estructura federal única de beneficiarios reales.

8.3 IMPLICACIONES JURÍDICO-DOGMÁTICAS DE LA IDENTIFICACIÓN DEL TITULAR REAL

Desde el punto de vista dogmático, el Reglamento (UE) 2024/1624 no es el mero refuerzo de la transparencia formal, en la medida en que incide de manera directa en el desarrollo estructural del concepto de titularidad real. Con ello se consigue desplazar la prioridad desde una perspectiva simplemente registral hacia un principio material basada en la supervisión efectiva.

Desde el punto de vista del Derecho penal económico, es bastante relevante el cambio, puesto que reduce los espacios de imputación indefinida que son propios de las organizaciones societarias complejas. Cuando se solicita la identificación del titular real atendiendo tanto a la propiedad como a la supervisión, el Reglamento establece un criterio funcional que simplifica la atribución jurídica de responsabilidad. Es especialmente en

[14] Financial Crimes Enforcement Network. (2025). *Beneficial Ownership Information Reporting. U.S. Department of the Treasury*. https://www.fincen.gov/boi
[15] Weiner, A. J., Montgomery, B. H., Thoren-Peden, D. S., Robbins, R. B., Patay, C. H., Keyko, D. G., & Yee, S. D. (2026). *CTA Update: A review of the status of beneficial ownership reporting requirements under the Corporate Transparency Act and related initiatives as of January 5, 2026*. Pillsbury Winthrop Shaw Pittman LLP. https://www.pillsburylaw.com/en/news-and-insights/cta-update.html

delitos de BC donde la ocultación del beneficiario final constituye un elemento típico central.

En este mismo sentido, la exigencia de que la información sobre titularidad real sea apropiada, exacta y actualizada, junto con la obligación de notificación dentro de un plazo máximo de 28 días (art. 63), no solo tiene un aspecto administrativo, además causa efectos directos sobre la eficacia probatoria en el proceso penal. Con este propósito, los registros de titularidad real se afirman como verdaderos instrumentos de estudio del *iter criminis* financiero. Esta situación contribuye a limitar el riesgo en la fase de investigación y facilitando la trazabilidad jurídica de los fondos ilícitos.

La ampliación del contenido informativo (art. 62), que incluye la naturaleza y extensión del interés real y el análisis de estructuras complejas, introduce por su parte un aspecto fundamental desde la dogmática del blanqueo. Ello da la posibilidad de relacionar jurídicamente la titularidad económica con la apariencia formal de legalidad. Esta relación es esencial para eludir los límites convencionales del Derecho penal frente a aspectos de estratificación y segregación patrimonial, elementos comunes del blanqueo mediante criptoactivos.

En conformidad con este enfoque, la Directiva (UE) 2024/1640 refuerza la configuración de los sistemas de acceso y centralización de la información. De este modo, se establece una perspectiva que va más allá de la simple armonización normativa al pasar a un marco jurídico de transparencia a nivel supranacional. Este desarrollo implica una optimización del principio de cooperación administrativa y judicial en la UE, principio esencial en un entorno de criminalidad transnacional.

Podemos afirmar que, el conjunto de estas normas genera las condiciones para sostener el modelo europeo al regirse por una lógica preventivo-estructural, orientada no únicamente a sancionar conductas, sino a limitar *ex-ante* las condiciones de posibilidad del delito, limitando el uso de instrumentos societarios como mecanismos de opacidad.

El modelo de EE. UU, por el contrario, tiene significativas implicaciones para la teoría del Derecho. Debilitar el *Corporate Transparency Act* y mitigar las obligaciones de identificación del titular real implica un cambio hacia un sistema, como resultado de ello la opacidad societaria vuelve a ser un área de riesgo jurídico relevante. Dogmáticamente, esto complica la identificación del sujeto activo del delito y complica la imputación penal en estructuras complejas.

Esta postura pone de relieve una disparidad estructural entre ambos sistemas. Por un lado, la UE desarrolla un modelo basado en la identificación *ex ante* y en la trazabilidad jurídica. Por el contrario, los EE. UU, conserva una lógica mayoritariamente reactiva basada en el *enforcement*, en el que la intervención tiene lugar una vez que se ha producido el ilícito.

Desde un punto de vista crítico, esta divergencia no es solo técnica, sino que es reflejo de dos concepciones distintas del Derecho penal económico:

Un modelo europeo de prevención estructural y reducción del riesgo sistémico.

Un modelo norteamericano de reacción punitiva, de persecución del delito.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Realmente, el desarrollo normativo europeo evidencia un esfuerzo de resolver la convencional disparidad entre trazabilidad económica y atribución jurídica. Por el contrario, el modelo estadounidense sigue mostrando complicaciones para integrar ambos planos de forma coherente en el ámbito del BC.

8.4. ¿CÓMO SE REFUERZAN LOS MECANISMOS DE LOCALIZACIÓN DE CUENTAS Y LA SUPERVISIÓN EUROPEA PARA DETECTAR ESQUEMAS CON CRIPTOACTIVOS Y EMPRESAS CON ESTRUCTURAS OPACAS?

La Directiva (UE) 2024/1640 exige a los Estados miembros establecer mecanismos automatizados centralizados que permitan identificar en tiempo real a cualquier persona que sea titular o controle, entre otros productos, cuentas de criptoactivos, además de cuentas bancarias, de pago, cuentas de valores y cajas fuertes (Dir. (UE) 2024/1640 art.16.1).

Dichos mecanismos deben incluir información mínima sobre titular, representante, titular real y fechas de apertura y cierre, incluso para cuentas de criptoactivos, un identificador único y las fechas de apertura y cierre (Dir. (UE) 2024/1640 art.16.3.f). Igualmente, debe estar prevista su interconexión a través del sistema BARIS[16], que la Comisión debe establecer y gestionar, con el objetivo de la interconexión como muy tarde el 10-7-2029 (Dir. (UE) 2024/1640 art.16.6).

Este refuerzo se completa con la creación de AMLA[17] para supervisar y unificar la supervisión y hacer más eficaz el sistema europeo en la prevención de riesgos transfronterizos de PBC y FT (Rgto. (UE) 2024/1620; entrada en vigor general 1-7-2025), dentro del paquete legislativo europeo de 2024.

9. EFICACIA DEL MARCO REGULATORIO EN EL BLANQUEO DE CAPITALES MEDIANTE CRIPTOACTIVOS

La capacidad de prevenir, detectar, atribuir y sancionar el BC, visto desde una perspectiva de eficacia reguladora, resulta necesario examinar comparativamente dichos marcos, en la medida en que tiene que considerarse también en relación con los principios de legalidad y seguridad jurídica. La determinación de las conductas típicas y su investigación efectiva dependen de la precisión normativa y de la capacidad de adaptación del Derecho penal económico en entornos tecnológicos sofisticados.

El análisis de la eficacia de los marcos regulatorios en materia de BC mediante criptoactivos necesita superar un enfoque formal centrado en la existencia de normas. Su objetivo es atender a su capacidad real de prevenir, detectar y perseguir las conductas

[16] El *Bank Account Registers Interconnection System* (BARIS) es un sistema informático de alcance europeo diseñado para interconectar los registros nacionales de cuentas bancarias de los Estados miembros de la EU, permitiendo un acceso rápido, seguro y armonizado a la información financiera relevante para la prevención, detección, investigación y persecución de delitos graves, incluido el blanqueo de capitales y la financiación del terrorismo.

[17] La AMLA (*Anti-Money Laundering Authority* / Autoridad Europea de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo) es una agencia descentralizada de la EU, creada en 2024 y con sede en Fráncfort, cuyo objetivo es supervisar, coordinar y reforzar el cumplimiento de las normas europeas en materia de prevención del blanqueo de capitales (AML) y financiación del terrorismo (CFT).

ilícitas en un entorno sofisticado tecnológicamente, así como la dimensión internacional de este fenómeno. El grado de desarrollo normativo, también debe examinarse a partir de su operatividad práctica y su capacidad de adaptación a las dinámicas del ecosistema cripto.

Es posible identificar criterios jurídicos y operativos a partir de esta premisa, para valorar la eficacia de los sistemas de PBC en este ámbito.

9.1. CAPACIDAD DE PREVENCIÓN

Para que un sistema sea eficaz en las políticas de prevención y represión contra el BC, el primer pilar es la prevención. Este primer pilar se concreta principalmente en el ámbito de los criptoactivos, en las obligaciones de diligencia debida previstas en el artículo 13 de la Directiva (UE) 2015/849, de conocimiento del cliente (KYC) y de evaluación del riesgo que deben cumplir los VASP.

El modelo de la EU presenta un enfoque más sólido, un sistema armonizado con unas obligaciones definidas para los intermediarios, fortaleciendo la trazabilidad y restringiendo la seudonimidad. El modelo estadounidense, por el contrario, encuentra numerosas limitaciones operativas para establecer obligaciones uniformes, lo cual podría originar espacios de riesgo.

No obstante, la eficacia preventiva no solamente depende de la existencia de estas obligaciones, sino de una adecuada aplicación y supervisión.

9.2. CAPACIDAD DE DETECCIÓN

Resulta crucial para mitigar el BC la detección operaciones sospechosas. En el ámbito de las monedas digitales, esa habilidad se traduce en la utilización de instrumentos de análisis de *blockchain* y en la colaboración entre actores públicos y privados.

La trazabilidad o seguimiento técnico de estas operaciones en redes públicas posibiliten que esta no siempre implique una identificación efectiva de los participantes involucrados. La efectividad de las normativas regulatorias radica en la incorporación de capacidades técnicas en las autoridades y de la colaboración con organismos especializados.

9.3. CAPACIDAD DE ATRIBUCIÓN

Como se ha mencionado en el análisis de la titularidad real, la intensificación de los sistemas de identificación contemplados en el Reglamento (UE) 2024/1624 favorece a la superación de la clásica brecha entre trazabilidad técnica y atribución jurídica. En el BC a través de criptoactivos, uno de los principales desafíos estructurales que presenta, se encuentra en la separación entre la trazabilidad de las transacciones y la atribución jurídica a personas físicas o jurídicas específicas.

De esta manera, el requerimiento de información precisa, actualizada y funcionalmente completa sobre el beneficiario efectivo posibilita identificar puntos de conexión entre las transacciones registradas en sistemas descentralizados. Ejemplo de ello

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

es, la *blockchain* y sujetos jurídicos determinados, puesto que facilitan así la imputación penal en los supuestos de BC.

Desde el punto de vista dogmático, dichos mecanismos potencian la posibilidad de poder identificar al verdadero titular económico más allá de las construcciones formales, lo cual resulta de esencial relevancia para la conformación del elemento subjetivo del delito y para la acreditación del conocimiento sobre el origen ilícito de los fondos. De tal forma, la arquitectura normativa europea no solo refuerza la capacidad de detección, sino que incide de manera decisiva en la capacidad de atribución jurídica, superando uno de los principales déficits estructurales del sistema tradicional frente a las nuevas formas de criminalidad financiera basadas en criptoactivos.

Es necesario probar la existencia de operaciones sospechosas para que se investigue un delito, su relación con un determinado sujeto y el conocimiento del origen ilícito de los fondos. Las redes *blockchain*, junto con el uso de *mixers*, monedas de privacidad o estructuras de estratificación, dificulta esta tarea por la naturaleza seudónima de estas.

La eficacia de los marcos regulatorios depende de su capacidad para generar puntos de conexión entre el ámbito digital y el mundo jurídico mediante mecanismos de identificación y obligaciones de información.

9.4. CAPACIDAD DE EJECUCIÓN Y SANCIÓN

El último elemento de evaluación consiste en la facultad de investigar, sancionar y decomisar los activos ilícitos. Esta dimensión tiene características propias dentro del campo de los criptoactivos, como *blockchain*, la transferencia entre fronteras y la limitación operativa y técnica de su decomiso.

La concepción basada en el *enforcement*, de conformidad con el modelo estadounidense, se caracteriza por una fuerte capacidad de investigación y persecución penal. Este carácter reactivo, sin embargo, puede no ser suficiente si no se completa con medidas preventivas.

Por el contrario, observamos un refuerzo de la EU en sus instrumentos de supervisión mediante la creación de la AMLA, dependiendo la eficacia, de su capacidad para coordinar a las autoridades nacionales.

9.5. EVALUACIÓN COMPARADA DE LA EFICACIA

Este criterio nos evidencia una vez estudiados que, ninguno de los modelos por sí solo resulta plenamente eficaz. El sistema norteamericano tiene fortalezas en la sanción, pero carencias en la prevención estructural. Sin embargo, el modelo de la UE proporciona un marco más coherente y preventivo, aunque enfrenta un desafío estructural en su aplicación.

Para una eficacia de los marcos regulatorios no solo a través del desarrollo normativo, es necesario que interactúen la regulación, las capacidades tecnológicas, la cooperación internacional y la especialización institucional. La separación entre

planificación normativa y capacidad operativa está la problemática principal, lo que refuerza la necesidad de un enfoque integral y coordinado.

La necesidad de una evolución del Derecho penal económico pone de manifiesto que, posibilite compatibilizar la eficacia en la investigación con el respeto a las garantías fundamentales.

10. CONCLUSIONES

El análisis desarrollado a lo largo de este trabajo posibilita confirmar que la eficacia de los marcos regulatorios en materia de BC mediante criptoactivos no depende únicamente de su grado de desarrollo normativo. En este sentido, depende de su capacidad real para prevenir, detectar, atribuir y sancionar conductas ilícitas, al generar la condición para afirmar que, los criptoactivos, criptomonedas y activos virtuales dan pie a métodos singulares, gracias a su seudonimato y a la naturaleza global y descentralizada de la tecnología *blockchain*, fenómeno en expansión. Las OC explotan estas características a propósito, utilizando una combinación de ofuscación sofisticada (por ejemplo, *smurfing*, cartera de criptoactivos, servicios de mezcla, monedas privadas, puentes entre *blockchain*) y estructuras corporativas opacas.[18] Con ello se consigue fragmentar, mover y ocultar el rastro del fondo, de las transacciones y servicios de mezcla, monedas privadas y puentes, vehículos que son susceptibles de explotación ilícita para dar mayor opacidad a sus rastros. Esta combinación tecnológica y societaria evidencia que el uso ilícito de dichos entornos no es accidental, sino estratégico y deliberado. Los mercados de la *darknet* no obstante, son facilitadores en dichos casos, como resultado de ello ofrecen lugares para el comercio anónimo.

Desde el análisis realizado, puede afirmarse que el BC a través de los criptoactivos, desde el análisis realizado, es un fenómeno complejo. Se caracteriza por la interacción entre la infraestructura tecnológica del ecosistema digital, la dimensión internacional de las operaciones y la capacidad de adaptación de las OC. La existencia de marcos normativos en este sentido no basta para garantizar su eficacia.

EE. UU y EU ponen de relieve enfoques muy diferenciados con respecto a los estudios de sus modelos regulatorios. Mientras que el modelo estadounidense se basa en un enfoque basado en el *enforcement*, la capacidad de investigación y de sanción. Por el contrario, la EU ha desarrollado un sistema más armonizado, preventivo, orientado a limitar la seudonimidad y a reforzar la trazabilidad de las transacciones. Ambos modelos, ya sea en la prevención estructural o en la aplicación concreta de las normas tiene sus claras limitaciones.

La trazabilidad técnica de las transacciones, como se ha señalado, no siempre se traduce en una identificación efectiva de los sujetos implicados, lo que genera esenciales desafíos probatorios y limita la atribución jurídica del delito. Por ello, la eficacia del marco regulatorio no puede medirse únicamente por el grado de desarrollo normativo. Se

[18] Una sociedad opaca es una entidad jurídica cuya estructura de propiedad, control y beneficiarios reales está diseñada para ocultar la identidad de las personas que realmente poseen o controlan la empresa. Su característica esencial es la falta de transparencia, que impide conocer al titular real (*ultimate beneficial owner*, UBO).

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

debe evaluar desde la capacidad real de prevención, detección, atribución y sanción de las conductas ilícitas.

La idea de que la eficacia depende de la integración de mecanismos de supervisión, capacidades técnicas y cooperación internacional, corrobora esta realidad. El empleo de cartera de criptoactivos de terceros, servicios de *mixing*, monedas de privacidad o los mercados en la *darknet y deep web* evidencia que la problemática no está únicamente en la seudonimidad, sino en la combinación de factores tecnológicos, regulatorios e institucionales.

El esfuerzo institucional para la mitigación del BC a través de criptoactivos requiere un enfoque integral que combine regulación, tecnología y capacidad operativa, cerrando la brecha entre el diseño normativo y su aplicación efectiva. A través de esta interacción, facilite reforzar la prevención, detección y persecución en el entorno de los criptoactivos, en la medida en que ninguno de los modelos examinados, resultan plenamente eficaces por sí solos.

La principal contribución de este estudio consiste en haber identificado la desconexión entre trazabilidad tecnológica y atribución jurídica como eje central de las limitaciones actuales del sistema de prevención del BC en criptoactivos.

11. REFLEXIÓN FINAL

El estudio del BC a través de criptoactivos ponen de relieve un fenómeno que va más allá de las categorías tradicionales del derecho penal y de la regulación financiera. La evolución tecnológica ha traído consigo, no solo posibilidades de innovación y nuevas formas de circulación de valor. En consecuencia, abren posibilidades de generar espacios de riesgo con la dificultad de acoplar a los modelos normativos existentes.

Se evidencia con este estudio comparado que, ni un enfoque centrado en el *enforcement*, ni un modelo predominantemente preventivo bastan por sí solos, puesto que se hace necesario replantear los mecanismos convencionales de intervención jurídica. La capacidad de los sistemas jurídicos para ajustarse a un entorno marcado por la velocidad, la descentralización y la complejidad técnica, es el nuevo desafío al que nos vemos obligados a enfrentar, así como la necesidad de reglamentaciones más modernas.

En contexto de los criptoactivos al reflejar una tensión creciente entre trazabilidad técnica y atribución jurídica, entre regulación formal y eficacia operativa, el BC va más allá de las divergencias entre jurisdicciones. El nuevo rol de las instituciones obliga a replantear, la tensión surgida, la cooperación internacional y la integración de capacidades tecnológicas como elementos esenciales del sistema.

La respuesta institucional definitiva para mitigar este fenómeno no puede ser solo normativa, sino también y tecnológica. Con una aproximación integral se podrá acortar la distancia entre el desarrollo de las normas y su eficiente implementación, asegurando una respuesta jurídica coherente contra un fenómeno en continua evolución.

12. REFERENCIAS BIBLIOGRÁFICAS

Anggriawan, R., & Susila, M. (2024). Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations. *Novum Jus, 18(2)*. Disponible en: https://doi.org/10.14718/novumjus.2024.18.2.10 [Última consulta: 23/02/2026].

Akkoyun, A. G., & Çelik, M. E. (2022). Transnational Organized Crime and the UN Convention. *Frontiers in Law, 1, 9–21*. Disponible en: https://doi.org/10.6000/2817-2302.2022.01.02 [Última consulta: 23/02/2026].

Alessi Longa, F. (2025). Cryptocurrency and money laundering. *American Journal of Industrial and Business Management, 15(2), 362–371*. Disponible en: https://doi.org/10.4236/ajibm.2025.152017 [Última consulta: 23/02/2026].

Anguren, 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*, 44, Banco de España. Disponible en: https://doi.org/10.53479/30054 [Última consulta: 23/02/2026].

Arnone, G., Scirè, G., & Bivona, E. (2025). The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review. *Digital Finance, 7, 815–851*. Disponible en: https://doi.org/10.1007/s42521-025-00148-1 [Última consulta: 23/02/2026].

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review. *Electronics, 13(17), 3568*. Disponible en: https://doi.org/10.3390/electronics13173568 [Última consulta: 23/02/2026].

Baer, K., de Mooij, R., Hebous, S., & Keen, M. (2023). Taxing cryptocurrencies. *Oxford Review of Economic Policy, 39(3), 478–497*. Disponible en: https://doi.org/10.1093/oxrep/grad035 [Última consulta: 23/02/2026].

Béres, F., Seres, I. A., Benczúr, A. A., & Quintyne-Collins, M. (2021). Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users. *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 69–78*. Disponible en: https://doi.org/10.48550/arXiv.2005.14051 [Última consulta: 23/02/2026].

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access, 9, 61048–61073*. Disponible en: https://doi.org/10.1109/ACCESS.2021.3072849 [Última consulta: 23/02/2026].

Blanco Barón, C. (2025). La regulación de los criptoactivos: más allá de un problema de eficiencia. *Revista de Economía Institucional, 27(53), 133–186*. Disponible en: https://doi.org/10.18601/01245996.v27n53.07 [Última consulta: 23/02/2026].

Chiang, S. (2024). Crypto Is Increasingly Being Used for Money Laundering. CNBC. Disponible en: https://www.cnbc.com/2024/07/16/crypto-is-increasingly-being-used-for-money-laundering-chainalysis-says.html [Última consulta: 23/02/2026].

Cremers, C., Loss, J., & Wagner, B. (2024). A holistic security analysis of Monero transactions. In Advances in Cryptology – EUROCRYPT 2024 (pp. 129–159). *Springer*. Disponible en: https://doi.org/10.1007/978-3-031-58734-4_5 [Última consulta: 23/02/2026].

Enríquez Pérez, I. (2020). Organized crime and institutional fragility as conditioning factors for development. *Revista Facultad de Ciencias Económicas*, 28(1). Disponible en: https://doi.org/10.18359/rfce.3564 [Última consulta: 23/02/2026].

Farrukh, H., Zafar, S., Rehman, Z. U., Shah, A. A., & Alshammry, N. (2025). Blockchain-based fraud detection: A comparative systematic literature review of federated learning and machine learning approaches. *Electronics*, 14(24), 4952. Disponible en: https://doi.org/10.3390/electronics14244952 [Última consulta: 23/02/2026].

Fu, Q., Liu, J., Pan, S., & Yuen, T. H. (2025). SoK: A deep dive into AML techniques for blockchain cryptocurrencies. *In ACISP 2025*. Disponible en: https://doi.org/10.1007/978-981-96-9095-4_16 [Última consulta: 23/02/2026].

Gorjón, S. (2023). Las finanzas descentralizadas o los criptoactivos de última generación. *Boletín Económico 2023/T3*, art. 04. Disponible en: https://doi.org/10.53479/30650 [Última consulta: 23/02/2026].

Hemdani, M. G. K. (2025). Cryptocurrencies and the Dark Web: A Gateway to Money Laundering. In Cybercrime Unveiled: Technologies for Analysing Legal Complexity (pp. 217–247). *Springer*. Disponible en: https://doi.org/10.1007/978-3-031-80557-8_10 [Última consulta: 23/02/2026].

Hinojal, A. (2023). Criptomonedas y blanqueo de capitales. *Logos Guardia Civil, 1, 215–240*. Disponible en: revistacugc.es/article/view/5742 [Última consulta: 23/02/2026].

Holt, T. J., Lee, J. R., & Griffith, E. (2023). An Assessment of Cryptomixing Services in Online Illicit Markets. *Journal of Contemporary Criminal Justice*. Disponible en: https://doi.org/10.1177/10439862231158004 [Última consulta: 23/02/2026].

Hope Kanu, D. (2025). Regulation of cryptocurrency and its implication for financial stability: A qualitative analysis. *IJEBMR, 9(4)*. Disponible en: https://doi.org/10.51505/IJEBMR.2025.9416 [Última consulta: 23/02/2026].

Isolauri, E. A., & Ameer, I. (2023). Money laundering as a transnational business phenomenon: A systematic review and future agenda. *Critical Perspectives on International Business, 19(3), 426–468*. Disponible en: https://doi.org/10.1108/cpoib-10-2021-0088 [Última consulta: 23/02/2026].

Jordá, C., Píriz, C., & Giménez-Salinas, A. (2024). Los criptomercados ilícitos de tráfico de drogas en la Dark Web: un estudio exploratorio empírico. *Revista Española de Investigación Criminológica, 22(2)*. Disponible en: https://doi.org/10.46381/reic.v22i2.884 [Última consulta: 23/02/2026].

Kabra, S., & Gori, S. (2025). Combating Cryptocurrency Laundering by Organised Crime Groups through an Effective Regulatory Framework. *IIUM Law Journal, 33(1)*. Disponible en: https://doi.org/10.31436/iiumlj.v33i1.1007 [Última consulta: 23/02/2026].

Koelbing, M., Kieseberg, K., Çulha, C., Garn, B., & Simos, D. E. (2024). Modelling smurfing patterns in cryptocurrencies with integer partitions. *IET Blockchain*. Disponible en: https://doi.org/10.1049/blc2.12087 [Última consulta: 23/02/2026].

Langdale, J. (2024). Combatting money laundering in Southeast Asian and Australian casinos. En Financial Crime and the Law (pp. 225–245). *Springer*. Disponible en: https://doi.org/10.1007/978-3-031-59543-1_9 [Última consulta: 23/02/2026].

Legrand, T., & Leuprecht, C. (2021). Securing Cross-Border Collaboration: Transgovernmental Enforcement Networks. *Policy and Society*, 40(4), 565–586. Disponible en: https://doi.org/10.1080/14494035.2021.1975216 [Última consulta: 23/02/2026].

Lim, A., & Choi, K.-S. (2025). Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization. *International Journal of Cybersecurity Intelligence & Cybercrime, 8(2)*. Disponible en: https://doi.org/10.52306/2578-3289.1220 [Última consulta: 23/02/2026].

Lom, A., & Hashmall, R. (2021). *New FATF Guidance Released on Virtual Assets and VASPs*. Disponible en: https://www.nortonrosefulbright.com/en-us/knowledge/publications/024b3d80/new-fatf-guidance-released-on-virtual-assets-and-virtual-asset-service-providers [Última consulta: 23/02/2026].

Luna Galván, M., Luong, H. T., & Astolfi, E. (2021). El narcotráfico como crimen organizado: perspectiva transnacional y multidimensional. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 16(1)*. Disponible en: https://doi.org/10.18359/ries.5412 [Última consulta: 23/02/2026].

Medranda Morales, N., & Arcos Argudo, M. (2023). Criptoactivos y criptomonedas. En Blockchain, criptoactivos y metaverso (pp. 41–62). *Editorial Abya-Yala*. Disponible en: https://doi.org/10.17163/abyaups.6 [Última consulta: 23/02/2026].

Menacho-Inga, W. G., Proaño-Reyes, G., & Castro-Sánchez, F. (2025). El uso de criptomonedas y el lavado de activos en Ecuador. *Noesis, 7(esp2)*. Disponible en: https://doi.org/10.35381/noesisin.v7i2.620 [Última consulta: 23/02/2026].

Mollaahmetoğlu, M. B., & Baykut, C. (2021). *Financial Action Task Force's Updated Guidance* Disponible en: https://chambers.com/articles/financial-action-task-force-s-updated-guidance-virtual-assets-and-virtual-asset-service-providers [Última consulta: 23/02/2026].

Montoya Arrubla, E. (2025). *Mecanismos de control del lavado de criptoactivos*. Diálogos Punitivos. Disponible en: https://dialogospunitivos.com/wp-content/uploads/2025/04/Columna-de-interes-43.pdf [Última consulta: 23/02/2026].

Rodríguez-Valencia, L., et al. (2025). A systematic review of artificial intelligence applied to compliance: fraud detection in cryptocurrency transactions. *Journal of Risk and Financial Management, 18(11), 612*. Disponible en: https://doi.org/10.3390/jrfm18110612 [Última consulta: 23/02/2026].

Soltani, R., Zaman, M., Joshi, R., & Sampalli, S. (2022). Distributed Ledger Technologies and Their Applications: A Review. *Applied Sciences, 12(15), 7898.* Disponible en: https://doi.org/10.3390/app12157898 [Última consulta: 23/02/2026].

Sudan, H. K., Tai, A. M. Y., Kim, J., & Krausz, R. (2023). Decrypting the cryptomarkets. Drug Science, *Policy and Law, 9, 1–19*. Disponible en: https://doi.org/10.1177/20503245231215668 [Última consulta: 23/02/2026].

Teng, H.-W., Härdle, W. K., Osterrieder, J., Pele, D. T., Baals, L. J., Papavassiliou, V.,

Bolesta, K., Kabašinskas, A., Filipovska, O., Thomaidis, N. S., Moukas, A.-I., Goundar, S., Abdul Nasir, J., Weinberg, A. I., Arakelian, V., Truică, C.-O., Akar, M., Kabaklarlı, E., Apostol, E.-S., Iannario, M., Będowska-Sójka, B., Skaftadóttir, H. K., Yildirim, O., Shala, A., Pisoni, G., Coita, I. F., Korba, S., Hafner, C. M., Schwendner, P., Molnár, B., & Xhumari, E. (2026). Digital assets: risks, regulations, mitigation. *Financial Innovation, 12, 65*. Disponible en: https://doi.org/10.1186/s40854-025-00848-y [Última consulta: 23/02/2026].

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science, 11(1)*. Disponible en: https://doi.org/10.1186/s40163-021-00163-8 [Última consulta: 23/02/2026].

Wang, H.-M., & Hsieh, M.-L. (2023). Cryptocurrency is new vogue: a reflection on money laundering prevention. *Security Journal, 37, 25–46*. Disponible en: https://doi.org/10.1057/s41284-023-00366-5 [Última consulta: 23/02/2026].

Warren, E., & Marshall, R. (2022). *Digital Asset Anti-Money Laundering Act of 2022 (S.5267)*. Senate of the United States. Disponible en: https://www.congress.gov/bill/117th-congress/senate-bill/5267 [Última consulta: 23/02/2026].

13. INFORMES DE ORGANISMOS

AMLC. (2023). *Analysis of Suspicious Transactions Associated with Casino Junkets*. Disponible en: http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf [Última consulta: 23/02/2026].

DEA. (2025). *National Drug Threat Assessment 2025*. Disponible en: https://www.dea.gov/documents/2025/2025-05/2025-05-13/national-drug-threat-assessment [Última consulta: 23/02/2026].

Europol. (2024). *Cryptocurrencies – Tracing the Evolution of Criminal Finances*. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [Última consulta: 23/02/2026].

Europol. (2022). Cryptocurrencies: Tracing the evolution of criminal finances. *Europol Spotlight Series*. Disponible en: https://doi.org/10.2813/75468 [Última consulta: 23/02/2026].

FATF, Egmont Group, INTERPOL, & UNODC. (2025). *International cooperation on money laundering detection, investigation and prosecution: Handbook*. Paris: FATF. Disponible en: https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html [Última consulta: 23/02/2026].

FATF. (2024). *Virtual assets: FATF standards and implementation*. FATF. Disponible en: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Última consulta: 23/02/2026].

FATF. (2023). *Targeted Update on Implementation of FATF Standards on Virtual Assets and VASPs*. FATF. Disponible en: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [Última consulta: 23/02/2026].

FATF.1. (2023). *Virtual Assets: Global* FATF Standards. Disponible en: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Última consulta: 23/02/2026].

FATF. (2022). *Money Laundering from Fentanyl and Synthetic Opioids*. Disponible en: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.coredownload.inline.pdf [Última consulta: 23/02/2026].

FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs.* Disponible en: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf [Última consulta: 23/02/2026].

FinCEN. (2025). *Advisory on Chinese Money Laundering Networks*. Disponible en: https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering [Última consulta: 23/02/2026].

Ministerio del Interior. (2024, 15 de noviembre). *Operación conjunta de la Policía Nacional y la Nationale Politie de Países Bajos (método OTC)* Disponible en:

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16371# [Última consulta: 23/02/2026].

NYDFS. New York State Department of Financial Services. (2024–2026). *Virtual Currency Business Licensing.* Disponible en: https://www.dfs.ny.gov/virtual_currency_businesses [Última consulta: 23/02/2026].

UNODC. (2026). *Global Programme on Cybercrime (capacity building materials)*. Capacidades/capacitación cripto/darknet/digital evidence: Disponible en: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/capacitybuilding.html. Catálogo de formación 2024: https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf [Última consulta: 23/02/2026].

UNODC. (2025). *Inflection Point: Global Implications of Scam Centers, Underground Banking and Illicit Online Marketplaces.* Disponible en: https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html [Última consulta: 23/02/2026].

UNODC. (2024). *Annual Report 2024: Organized Crime Section. United Nations Office on Drugs and Crime*. Disponible en: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Última consulta: 23/02/2026].

UNODC.1. (2024). *Criminal Networks and Fragmented Structures*. Disponible en: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Última consulta: 23/02/2026].

UNODC.2. (2024). *Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. Disponible en: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf [Última consulta: 23/02/2026].

U.S. Department of Justice. (2023). *United States v. Binance Holdings Limited, d/b/a Binance.com (case overview).* Disponible en: https://www.justice.gov/criminal/case/united-states-v-binance-holdings-limited-dba-binancecom [Última consulta: 23/02/2026].

U.S. Department of Justice.1. (2023). *United States v. Changpeng Zhao (case overview)*. Disponible en: https://www.justice.gov/criminal/case/united-states-v-changpeng-zhao [Última consulta: 23/02/2026].

14. LEGISLACIÓN

Consejo de la Unión Europea. (2024) Directiva (UE) 2024/1640 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, por la que se modifica la Directiva (UE) 2019/1937 y se modifica y deroga la Directiva (UE) 2015/849. DOUE L 2024/1640, de 19 de junio de 2024.

Organización de las Naciones Unidas. (2000). Naciones Unidas. (2000). Convención de las Naciones Unidas contra la delincuencia organizada transnacional (Resolución A/RES/55/25).

Parlamento Europeo. (2024). Sexta Directiva antiblanqueo. Resolución legislativa del Parlamento Europeo, de 24 de abril de 2024, sobre la propuesta de Directiva relativa a los mecanismos para prevenir el uso del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se deroga la Directiva (UE) 2015/849. DOUE C/2025/3790, 17 de septiembre de 2025.

Parlamento Europeo y Consejo de la Unión. (2024) 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. DOUE L 2024/1624, 19 de junio de 2024.

Parlamento Europeo y Consejo de la Unión. (2024) Reglamento (UE) 2024/1620 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010. DOUE L 2024/1620, 19 de junio de 2024

Parlamento Europeo y Consejo de la Unión. (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. DOUE, L 150, 9 de junio de 2023.

United States Congress. (1977). International Emergency Economic Powers Act, Pub. L. No. 95-223, 91 Stat. 1625–1629 (codified as amended at 50 U.S.C. §§ 1701–1707).

United States Congress. (1970). Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114

(codified as amended at 31 U.S.C. §§ 5311–5336).

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

15. OTRAS FUENTES NO CIENTÍFICAS

Binance Academy. (2024). ¿Qué es la minería de criptomonedas o criptominería y cómo funciona? Binance. Disponible en: https://www.binance.com/es/academy/articles/what-is-crypto-mining-and-how-does-it-work [Última consulta: 23/02/2026].

Chainalysis. (2025). 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized. Disponible en: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ [Última consulta: 23/02/2026].

Coinmetro Editorial Team. (2024, agosto 2). Crypto Mixers: Privacy Tools and Regulatory Challenges. *Coinmetro*. Disponible en: https://coinmetro.com/learning-lab/crypto-mixers-privacy-tools-and-regulatory-challenges [Última consulta: 23/02/2026].

Elliptic. (2024). *Preventing Financial Crime in Cryptoassets: Typologies Report*. https://www.elliptic.co/hubfs/Elliptic%20Typologies%20Report%202024.pdf [Última consulta: 23/02/2026].

16. DECLARACIÓN DE INTEGRIDAD ACADÉMICA Y CIENTÍFICA

Que constituye un trabajo original, realizado por mí, sin plagio ni uso indebido de trabajos ajenos, conforme a los estándares internacionales de integridad académica y científica.

Los datos, resultados y conclusiones han sido obtenidos y tratados de forma honesta y rigurosa, sin fabricación, falsificación ni manipulación indebida.

El uso de la inteligencia artificial o de otras herramientas digitales se ha ajustado la normativa universitaria, sin sustituir la autoría intelectual ni el juicio académico propio.

No existen conflictos de interés que haya influido en el desarrollo o los resultados de la investigación.

Soy consciente de que el incumplimiento de estas declaraciones puede dar lugar a la anulación del título de doctor a las responsabilidades académicas o legales que correspondan.

A sí mismo, ASUMO cualquier responsabilidad derivada del incumplimiento del compromiso ético recogido en esta declaración.