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

Artigo de Investigação

BRANQUEAMENTO DE CAPITAIS ATRAVÉS DE CRIPTOATIVOS: EFICÁCIA REGULATÓRIA E DISCREPÂNCIA ENTRE RASTREABILIDADE TECNOLÓGICA E ATRIBUIÇÃO JURÍDICA NA UNIÃO EUROPEIA E NOS ESTADOS UNIDOS

Tradução para o português com ajuda de IA (DeepL)

Benjamín Garcinuño Roldán
Doutorando na Escola Internacional de Doutoramento da UNED (EIDUNED), membro da Guardia Civil, advogado inscrito na Ordem dos Advogados de Córdoba. Mestre em Segurança, Licenciado em Direito
bgarcinun2@alumno.uned.es
https://orcid.org/0009-0005-6923-1004

Recebido em 25/02/2026
Aceite em 02/06/2026
Publicado em 30/06/2026

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

Citação recomendada: Garcinuño B. (2026). Branqueamento de capitais através de criptoativos: eficácia regulatória e discrepância entre rastreabilidade tecnológica e atribuição jurídica na União Europeia e nos Estados Unidos. *Revista Logos Guardia Civil*, 4(2), pp. 215-252. https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Registo Legal: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

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

DEDICATÓRIA

À Mariam, por confiar em mim,
e por alimentar os pássaros da minha cabeça.
Tenho de lhe lembrar que o sol continua a brilhar, mesmo que não o veja.

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

BRANQUEAMENTO DE CAPITAIS ATRAVÉS DE CRIPTOATIVOS: EFICÁCIA REGULATÓRIA E DISCREPÂNCIA ENTRE RASTREABILIDADE TECNOLÓGICA E ATRIBUIÇÃO JURÍDICA NA UNIÃO EUROPEIA E NOS ESTADOS UNIDOS

Resumo: A lavagem de capitais é um fenómeno dinâmico cuja evolução está ligada ao contexto económico internacional. Os métodos de lavagem de capitais ilícitos geram novos desafios regulamentares e operacionais para as autoridades e as entidades financeiras, em grande parte impulsionados pelo desenvolvimento da tecnologia. Com o uso de certas tecnologias recentes, criam um ambiente de pseudonimidade, que transcende a sua natureza meramente técnica. Esta característica funciona como um instrumento estratégico para as organizações e grupos criminosos (OC) que procuram sofisticar os seus esquemas de branqueamento, permitindo ocultar a rastreabilidade e as consequências dos danos subjacentes**.** O presente artigo analisa criticamente a problemática do branqueamento de fundos ilícitos através de criptoativos por parte dos OC e as diversas estratégias que estes empregam para ocultar a sua rastreabilidade e identidade. Em primeiro lugar, examinam-se de forma sistemática os instrumentos internacionais, tais como a Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional e as recomendações do Grupo de Ação Financeira

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

Internacional (GAFI) no que diz re e ao sistema de repressão e prevenção da lavagem de fundos ilícitos por meio de criptoativos. Partindo deste quadro internacional, o presente trabalho articula-se em torno de uma análise comparativa do quadro legislativo, substancialmente diferente no que diz respeito à lavagem de capitais através de criptoativos nos Estados Unidos (EUA) e na União Europeia (UE). O presente estudo não se limita a uma abordagem descritiva do fenómeno, mas aponta para a necessidade de reforçar a arquitetura regulatória, através da identificação de divergências legislativas significativas, lacunas jurídicas e limitações nos mecanismos de supervisão.

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 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.

Palavras-chave: Criptoativos, branqueamento de capitais, criminalidade organizada, pseudonimidade digital, regulamentação financeira, tecnologias emergentes, darknet, transparência e titularidade real.

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

ABREVIATURAS

AML: *Anti-Money Laundering*. Em português: combate ao branqueamento de capitais.

AMLA: *Anti-Money Laundering Authority*. Em português: Autoridade Europeia de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

AMLC: *Anti-Money Laundering Council*. Em português: Conselho contra a lavagem de capitais ou de dinheiro.

BARIS: *Sistema de Interconexão de Registos de Contas Bancárias.* Em espanhol: Sistema de Interconexão de Registos de Contas Bancárias da União Europeia.

BC: Branqueamento de capitais.

BSA: *Bank Secrecy Act.* Em português: Lei do Sigilo Bancário.

CDD: *Customer Due Diligence*. Em português: Diligência Devida em relação ao Cliente (DDC).

CEO: *Chief Executive Officer*. Em português: diretor executivo ou administrador delegado, consoante o país.

CFT: *Combate ao Financiamento do Terrorismo*. Em espanhol: Luta contra o Financiamento do Terrorismo.

CFTC: *Commodity Futures Trading Commission*. Em português: a agência federal independente dos Estados Unidos que regula os mercados de derivados (futuros, *swaps* e certas opções).

DAO: *Decentralized Autonomous Organization*. Em português: no contexto da lavagem de capitais (AML/CFT), é uma organização nativa da *blockchain* que coordena decisões e gere ativos através de *contratos inteligentes* e governação por tokens, sem uma direção central tradicional.

DEA: *Drug Enforcement Administration*. Em português: Administração para o Controlo de Drogas.

EUA: Estados Unidos.

EUR: Moeda euro.

FATF: *Financial Action Task Force*. Em português: GAFI.

FBI: *Federal Bureau of Investigation*. Em português: é a Agência Federal de Inteligência e Segurança Interna dos Estados Unidos e o seu principal órgão policial federal.

FinCEN: *Financial Crimes Enforcement Network.* Em português, costuma ser traduzida como Rede de Controlo/Execução de Crimes Financeiros.

FT: Financiamento do terrorismo.

GAFI: Grupo de Ação Financeira Internacional.

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

IA: Inteligência artificial.

IEEPA: *International Emergency Economic Powers Act*. Em português: Lei dos Poderes Económicos em Emergências Internacionais.

ICO: *Initial Coin Offering*. Em espanhol: Oferta Inicial de Moedas.

IRS: *Internal Revenue Service*. Em português, a Agência Federal de Recolha de Impostos dos Estados Unidos.

KYC: *Know Your Customer*. Em espanhol: Conheça o seu cliente.

MiCA: *Markets in Crypto-Assets*. Em português: Regulamento dos Mercados de Criptoativos.

NCA: *National Crime Agency*. Em português: Agência Nacional contra o Crime do Reino Unido.

NYDFS: *Departamento de Serviços Financeiros do Estado de Nova Iorque*. Em português: Departamento de Serviços Financeiros do Estado de Nova Iorque.

OC: Organização criminosa.

PBC/FT: Prevenção do branqueamento de capitais e do financiamento do terrorismo.

SEC: *Securities and Exchange Commission*. Em português: Comissão de Valores Mobiliários dos Estados Unidos.

SEPBLAC: Serviço Executivo da Comissão de Prevenção da Lavagem de Dinheiro e Infrações Monetárias.

STR: *Relatório de Transação Suspeita*. Em espanhol: Reporte de Transacción Sospechosa.

UIF: Unidade de Inteligência Financeira. É o SEPBLAC em Espanha (Serviço Executivo da Comissão de Prevenção do Branqueamento de Capitais e Infrações Monetárias).

UNODC: *United Nations Office on Drugs and Crime*. Em português: Gabinete das Nações Unidas contra a Droga e o Crime.

UNTOC: *Convenção das Nações Unidas contra o Crime Organizado Transnacional*. Em espanhol: Convenção das Nações Unidas contra o Crime Organizado Transnacional.

USD: *Dólar dos Estados Unidos*, ou dólar americano.

VASP: *Virtual Asset Service Provider*. Em português: Prestadores de Serviços de Ativos Virtuais ou CASP no âmbito europeu.

6AMLD: Sexta Diretiva relativa à Luta contra o Branqueamento de Capitais e o Financiamento do Terrorismo.

1. INTRODUÇÃO

Nos últimos anos, os criptoativos revolucionaram o mundo das finanças, abrindo portas para a inovação e a inclusão financeira como nunca antes se tinha visto. Mas este progresso tecnológico também deu origem a novos desafios, especialmente no domínio da criminalidade financeira. Uma das questões mais preocupantes é a utilização de criptoativos para a lavagem de capitais (LC) por parte de organizações ou grupos criminosos (OC).

Esses ativos operam geralmente em redes descentralizadas denominadas «*blockchains*», que garantem transações transparentes e seguras sem a necessidade de um terceiro centralizado, como um banco (Bhutta et al., 2021). Ao transferir uma criptomoeda, a transação é registada na *blockchain*, que funciona como um livro-razão público distribuído por muitos computadores em todo o mundo. (Soltani et al., 2022) As transações são verificadas por uma rede de utilizadores conhecidos como «mineradores», que são recompensados com novas unidades de criptoativos (Binance Academy, 2024).

Durante décadas, a lavagem de dinheiro (BC) tem sido um problema a nível internacional. A ocultação da proveniência dos fundos obtidos ilegalmente tem sido o principal objetivo das organizações criminosas (OC), com o firme propósito de lhes conferir uma aparência legal nos sistemas económicos. As OC podiam, com esta técnica, investir os seus lucros ilegais sem deixar rastros financeiros que pudessem levar à sua descoberta e processo judicial.

As OC convencionais são altamente estruturadas, com hierarquias e funções definidas para os seus membros (Enríquez Pérez, 2020); são frequentemente apoiadas por políticos locais e recorrem à corrupção para evitar problemas com a polícia (Luna Galván et al., 2021). Operam através de estruturas descentralizadas que dificultam a identificação das suas atividades (UNODC, 2024). A estrutura dessas OC é concebida para as proteger das forças da ordem e reduzir o risco de infiltração ou traição (UNODC.1, 2024). Para garantir uma definição comum de criminalidade organizada entre os Estados-Membros, foi criada a Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional. A presente Convenção define uma OC como um grupo estruturado de três ou mais pessoas que atuam em conjunto para cometer crimes com o objetivo de obter um benefício financeiro direto ou indireto (Akkoyun & Çelik, 2022).

As OC, com um elevado nível de especialização na utilização de ferramentas financeiras complexas, recorrem cada vez mais às moedas virtuais para dissimular a origem dos seus fundos ilícitos (Trozze et al., 2022). As OC utilizam técnicas como o *layering*[1] , os serviços de mistura e as transferências transfronteiriças para dificultar a rastreabilidade dos fundos. (Arnone et al., 2025). A incorporação de ferramentas de análise *de blockchain* e o reforço das obrigações KYC/PBC/FT (Prevenção do Branqueamento de Capitais e do Financiamento do Terrorismo) permitem otimizar a deteção e o controlo de operações ilícitas. (Rodríguez-Valencia et al., 2025).

[1] O *layering* (ou estratificação) é a segunda fase do processo de branqueamento de capitais, na qual o objetivo principal é ocultar a origem ilícita dos fundos através de uma série de transações financeiras complexas, sucessivas e, frequentemente, transfronteiriças. Esta etapa visa interromper a rastreabilidade do dinheiro e dificultar que as autoridades possam reconstruir o percurso original dos fundos.

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

O artigo que se segue aborda a problemática da lavagem de fundos ilícitos através de criptoativos por parte das OC e o quadro jurídico existente para a combater. A análise inclui as recomendações do GAFI, os instrumentos internacionais e as regulamentações dos Estados Unidos (EUA) e da União Europeia (UE) para prevenir a lavagem de dinheiro com criptoativos por parte das OC. O presente trabalho examina os tratados internacionais e as leis nacionais dos EUA e da Europa que visam prevenir a lavagem de dinheiro por parte das OC.

Partindo desta premissa, desenvolvemos, no presente artigo, uma análise comparativa dos modelos regulamentares dos EUA e da UE, com o objetivo de identificar os seus pontos fortes e fracos e formular critérios jurídicos de avaliação. Da mesma forma, o presente trabalho defende a eficácia do esforço institucional para a mitigação da lavagem de dinheiro através de criptoativos, uma vez que não depende exclusivamente do desenvolvimento formal dos quadros normativos. Além disso, o seu grau de eficácia depende da capacidade real de prevenir, detetar, atribuir e sancionar condutas ilícitas num ambiente caracterizado pela pseudonimidade, pela descentralização tecnológica e pela dimensão transnacional do fenómeno.

A principal contribuição reside na identificação da existência de uma lacuna estrutural entre a rastreabilidade técnica das transações na *blockchain* e a sua atribuição jurídica efetiva; esta é a principal contribuição deste estudo. Consequentemente, os modelos convencionais de prevenção, deteção e sanção, que incorporam capacidades tecnológicas nos sistemas regulatórios, devem ser repensados.

2. METODOLOGIA DE INVESTIGAÇÃO

O presente documento utiliza uma abordagem analítica descritiva. A análise será multidimensional, abordando a legislação, a literatura e a informação para avaliar as medidas de prevenção do branqueamento de criptoativos por parte das OC. A revisão exploratória da literatura já existente (livros, revistas, artigos, etc.) proporcionará uma melhor compreensão do conceito, da forma e das melhores formas de resolver esta problemática.

Esta abordagem constitui a metodologia mais adequada para desenvolver a investigação, devido à escassez de informação e à inexistência de artigos que abordem de forma exaustiva as recomendações do GAFI, as convenções internacionais e as legislações nacionais dos EUA e da Europa sobre a problemática da lavagem de criptoativos por parte das OC.

Além disso, o trabalho incorpora uma dimensão analítica de caráter propositivo, orientada para identificar as limitações estruturais do atual quadro jurídico em ambientes digitais descentralizados.

3. ANÁLISE DA UTILIZAÇÃO (INDEVIDA) DE CRIPTOATIVOS POR PARTE DE ORGANIZAÇÕES CRIMINOSAS

A proliferação de serviços bancários clandestinos e outras redes de branqueamento de capitais online gerou canais de transferência financeira mais anónimos (Europol, 2022). Os criptoativos têm potencial para serem utilizados indevidamente por criminosos; em

consequênci , a indústria está a desenvolver novas formas complexas e serviços de mistura entre pares. Isto cria as condições para ocultar transações, a análise regular descentralizada da *blockchain* e as novas redes peer-to-peer que surgiram recentemente e que provavelmente serão utilizadas em atividades ilegais (Hinojal, 2023). Tais desenvolvimentos limitarão significativamente a identificação de atividades das OC que utilizam criptomoedas convencionais para encobrir ganhos ilícitos (Fu et al., 2025).

O tráfico de droga, de armas e de outras mercadorias ilegais é um negócio lucrativo, na medida em que permite movimentar facilmente fundos ilícitos de e para organizações criminosas em qualquer parte do mundo (Sudan et al., 2023). De facto, para além dos esquemas fraudulentos, os criptoativos têm sido associados a quase todos os tipos de crimes cibernéticos, desde serviços na *deep web*[2] ou *na darknet*[3] até ao roubo e à fraude nas suas diversas formas.

Os criptoativos têm sido utilizados numa variedade de atividades das organizações criminosas (OC), incluindo branqueamento de capitais, ataques *de ransomware*[4] e fraude online. Com o objetivo de combater estas práticas ilícitas, foi fornecida às forças da ordem uma visão geral da literatura existente sobre o tema (Trozze et al., 2022). A investigação sobre a utilização indevida por parte das OC ainda é escassa em comparação com outros temas de investigação sobre criptoativos e *blockchain*. Entre as atividades ilegais realizadas pelas OC com moedas digitais encontram-se a lavagem de dinheiro (produto de crimes), o *ransomware* e os mercados negros (Alessi Longa, 2025).

Foram identificadas sete categorias, cada uma das quais resume um padrão específico de comportamento criminoso na utilização dos criptoativos e as suas implicações para os mecanismos de prevenção, deteção e resposta:

(1) O financiamento do terrorismo, (2) na BC, (3) nos mercados da *deep web* ou *darknet*, (4) na cibercriminalidade, (5) no tráfico de drogas, (6) no tráfico de pessoas, (7) e na corrupção.

Iremos centrar a nossa investigação na opção 2:

4. CRIPTOATIVOS E BRANQUEAMENTO DE CAPITAIS POR PARTE DOS GRUPOS CRIMINOSOS ORGANIZADOS

Os criptoativos recebidos por endereços ilícitos em 2023 ascenderam a 46 100 milhões de dólares americanos (Chainalysis, 2025). Em 2024, o valor recebido por endereços ilícitos desceu para 40 900 milhões de dólares. No entanto, os números de 2024 são

[2] A deep web (ou web profunda) é a parte da Internet que não está indexada pelos motores de busca convencionais, como o Google, o Bing ou o Yahoo. Isto significa que o seu conteúdo não pode ser encontrado através de pesquisas normais e só é acessível se se conhecer diretamente o endereço, se se tiver autorização ou se se utilizarem credenciais específicas.

[3] A darknet é uma parte específica e deliberadamente oculta da Internet, à qual só se pode aceder através de software, configurações ou protocolos especiais que proporcionam anonimato, como o Tor, o I2P ou o Freenet. Não está indexada pelos motores de busca convencionais e foi concebida para proteger a identidade e a localização dos utilizadores e dos servidores.

[4] O *ransomware* é um tipo de software malicioso (*malware*) concebido para bloquear, encriptar ou inutilizar os sistemas informáticos de uma vítima, com o objetivo de exigir um resgate financeiro — geralmente em criptomoedas — em troca da recuperação do acesso aos dados ou sistemas.

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

provisórios e poderão facilmente ultrapassar os 51 000 milhões de dólares (Atlam et al., 2024).

Embora alguns afirmem que os criptoativos envolvem elevados custos de informação e controlo, em geral as transações são mais baratas e rápidas do que as transações em moedas fiduciárias, uma vez que não existem intermediários entre compradores e vendedores (Medranda Morales & Arcos Argudo, 2023). No entanto, estas mesmas características têm sido aproveitadas pelas organizações criminosas para a lavagem de dinheiro. Em particular, três características dos criptoativos reduzem drasticamente os custos de transação destas atividades ilegais.

Em primeiro lugar, a natureza descentralizada dos criptoativos permite que os utilizadores troquem valor diretamente entre si, sem necessidade de intermediários. Como já foi referido, as normas tradicionais destinadas a combater a lavagem de dinheiro visam regulamentar os intermediários que realizam operações para prevenir transferências ilegais (Longa, 2025) e a ausência de interações presenciais nas transações com criptoativos torna mais difícil a identificação das partes envolvidas (Montoya Arrubla, 2025). Em segundo lugar, embora todas as transações fiquem registadas e sejam rastreáveis na *blockchain*, não existe uma ligação explícita com indivíduos ou organizações reais por trás delas. Os criptoativos funcionam num sistema pseudónimo em que apenas se conhece a chave pública (uma sequência aleatória de números), mas a chave privada é mantida em segredo.

Isto dificulta significativamente a associação de uma identidade real a um endereço de criptomoeda (Béres et al., 2021). No entanto, os utilizadores podem criar várias carteiras de criptoativos eletrónicos com endereços públicos diferentes, o que dificulta a rastreabilidade em caso de suspeita de branqueamento de capitais (Atlam et al., 2024).

Por fim, a rapidez das transações com criptoativos e a sua facilidade de utilização conferem uma vantagem em relação aos métodos tradicionais de branqueamento de capitais, como o dinheiro em numerário. Ao contrário do dinheiro em papel, que está limitado pelo peso e pelo tamanho, os criptoativos podem ser armazenados em quantidades ilimitadas numa pen USB e enviados para qualquer pessoa no mundo em questão de minutos. A maleabilidade das transações facilita a evasão das medidas regulatórias, uma vez que permite dividir uma transação de grande valor em outras mais pequenas (Koelbing et al., 2024). Esta flexibilidade operacional é vital e reforça o BC para as OC que operam nos mercados de criptoativos. Estas organizações geram um grande volume de criptoativos, que precisam de transformar em fundos com aparência legal.

Este processo envolve geralmente uma série de transações financeiras complexas que movimentam os fundos através de múltiplas contas e jurisdições, tornando difícil rastrear a origem dos fundos. O que permite às OC continuar a operar na ilegalidade e ocultar os lucros do tráfico de droga (FATF, 2022). As OC que utilizam a *deep web* são especialistas na lavagem de criptoativos, os quais podem ser transferidos instantaneamente de uma conta para outra e são difíceis de rastrear (Holt et al., 2023). Essas OC contratam frequentemente facilitadores profissionais (advogados, contabilistas, banqueiros, etc.) para dificultar a rastreabilidade dos seus fundos ilícitos.

As OC podem reter como investimento os criptoativos que recebem nas operações do mercado de criptomoedas. Estes são utilizados para branquear outras moedas ilícitas, tanto online como no mundo real (Arnone et al., 2025). Os que não são mantidos como investimento são branqueados e introduzidos na economia legal. Por exemplo, a polícia holandesa descobriu que um moderador de um mercado de criptomoedas aproveitava os seus contactos para trocar bitcoins por dinheiro (Ministério do Interior, 2024).

Na Ásia Oriental e do Sudeste, as organizações denominadas «*point* runners» ou «*moving* ants» são utilizadas para branquear fundos ilícitos, recrutando muitas pessoas (muitas vezes jovens desempregados) que disponibilizam as suas contas bancárias e criam empresas fictícias para ocultar a origem e o destino dos fundos ilícitos (UNODC, 2025). Estas redes movimentam os fundos através de múltiplas contas bancárias ou de criptoativos e casinos online, onde são disfarçados como ganhos legítimos de casino (Langdale, 2024).

Agora que as autoridades têm um melhor conhecimento dos pagamentos por terceiros (na sequência da «*Operação Chain* Break» e de outras operações semelhantes na China) (FinCEN, 2025), os OC têm recorrido cada vez mais aos criptoativos para as suas operações de jogo ilegal, o que coloca sérios desafios aos investigadores (Europol, 2024). Por exemplo, os casinos e operadores de *junkets*[5] licenciados nas Filipinas estiveram envolvidos na lavagem de cerca de 81 milhões de dólares subtraídos num ciberataque de 2016 atribuído ao grupo Lazarus do Banco Central do Bangladesh (Langdale, 2024). Embora o dinheiro tenha passado por bancos e empresas de remessas, foi extremamente complexo rastreá-lo assim que chegou às mãos dos operadores de viagens de jogo do casino (AMLC, 2023).

Os cartéis globais de droga foram acusados pela DEA de utilizar *a Binance*,[6] — por ser a maior plataforma de câmbio de criptomoedas — para branquear, em diversas transações, montantes entre 15 e 40 milhões de dólares (DEA, 2025). De acordo com os relatórios da DEA, *a Binance* está a colaborar com os investigadores no âmbito do inquérito relativo a várias denúncias.

Esses mecanismos sofisticados geram novos desafios para a sua deteção e investigação, devido ao número de transações e à sua natureza transfronteiriça, exigindo maior transparência financeira, cooperação internacional e quadros regulamentares mais sólidos para combater esses crimes (Legrand & Leuprecht, 2021).

[5] Os operadores de junkets são intermediários especializados que atuam entre os casinos e os jogadores VIP ou high-rollers, especialmente em mercados como Macau, Las Vegas, Singapura e outros centros internacionais de jogo. A sua função principal é recrutar, transportar, financiar e gerir clientes de alto valor para que joguem em determinados casinos.

[6] A Binance é a maior bolsa de criptomoedas do mundo em volume de negociação e número de utilizadores, fundada em 2017 por Changpeng Zhao (CZ) e Yi He. É uma plataforma centralizada (CEX) que permite comprar, vender, trocar e custodiar ativos digitais.

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

5. MÉTODOS MAIS COMUNS DE BRANQUEAMENTO DE CRIPTOATIVOS UTILIZADOS PELAS OC

5.1. CONSIDERAÇÕES GERAIS A PARTIR DA DOGMÁTICA DA LAVAGEM DE CAPITAIS

O fenómeno conceptualizado revela que as diferentes técnicas empregadas pelas OC se enquadram nas fases clássicas da lavagem de capitais, em particular a colocação, a estratificação e a integração.

São estas práticas, descritas na secção anterior, que geram as dificuldades relacionadas com a tipicidade, a atribuição de responsabilidade e a reconstruçã e do percurso financeiro dos fundos ilícitos. Especialmente num ambiente caracterizado pelo pseudonimato e pela descentralização tecnológica, como é o caso dos criptoativos.

5.2. TÉCNICAS RELACIONADAS COM A FASE DE INTEGRAÇÃO: O *SMURFING*

A prática conhecida como «*smurfing*», «pitufeo» ou «menudeo» implica a integração no sistema financeiro, de forma variada e em pequenas quantias, de fundos obtidos através de atividades ilícitas, moedas provenientes do tráfico de droga, pagamentos resultantes de fraude, corrupção ou lucros originários da exploração sexual (Isolauri & Ameer, 2023). Esta técnica, utilizada nas finanças convencionais, parece ter-se transferido para o mundo dos criptoativos (Koelbing et al., 2024).

Do ponto de vista do direito penal, este tipo de práticas pode enquadrar-se na fase de integração do BC. Deixamos claro que a intenção é introduzir fundos ilícitos no sistema financeiro oficial, através da sua fragmentação, para contornar os mecanismos de controlo. De uma perspetiva jurídica, isto levanta questões relevantes sobre a aplicação de limiares regulamentares e a eficácia dos sistemas de deteção automatizada.

5.3. TÉCNICAS RELACIONADAS COM A FASE DE ESTRATIFICAÇÃO: OCULTAÇÃO E DESASSOCIAÇÃO DA ORIGEM ILÍCITA

5.3.1. Carteira de criptoativos (carteiras médias) (medium wallets ou mid-size wallets)

Um método comum de BC com criptoativos implica a utilização de carteiras intermediárias. Esta técnica de estratificação visa dissimular a ligação entre os fundos ilícitos e a sua posterior entrada no sistema financeiro legal. (Elliptic, 2024). Consequentemente, as carteiras intermediárias estão a ser utilizadas por criminosos em plataformas *de câmbio* com e sem KYC.

Do ponto de vista dogmático, as contas intermediárias e a sua utilização estão diretamente ligadas à fase de estratificação da lavagem de dinheiro, uma vez que se destinam a dificultar a rastreabilidade dos fundos ilícitos. Estas condutas descritas geram desafios essenciais no que diz respeito à atribuição objetiva e à identificação do titular económico, em particular quando não existem pontos de contacto com intermediários obrigados a identificar.

5.3.2. Carteiras de criptoativos de consolidação

As carteiras de consolidação, que agrupam e combinam fundos de diversas fontes, constituem outra tendência a ter em conta. Este padrão de consolidação pode revelar tentativas de ocultar a origem ilícita dos fundos antes de os transferir para bolsas ou outros locais de levantamento de dinheiro (Chiang, 2024).

Estas estruturas, de um ponto de vista jurídico, poderiam ser consideradas como instrumentos concebidos para reforçar a ocultação da origem ilícita dos fundos. Esta circunstância afeta diretamente a configuração típica do crime de BC na sua modalidade de ocultação ou encobrimento.

5.3.3. Serviços de mistura, moedas de privacidade e pontes

O objetivo da mistura e da baralhada é separar as elevadas quantidades de moedas virtuais, distribuindo-as em múltiplas direções (Gorjón, 2023). Os misturadores são indivíduos ou empresas que distribuem os fundos entre os participantes e os misturam com rendimentos lícitos, com o objetivo de ocultar a rastreabilidade e a identificação dos proprietários (Equipa Editorial da Coinmetro, 2024).

As questões específicas relativas à tipicidade na fase de ocultação das moedas virtuais, suscitadas pela utilização de serviços de mistura, são concebidas precisamente para dificultar a rastreabilidade dos fundos. Consequentemente, esta problemática põe em causa o âmbito das obrigações de diligência devida dos prestadores de serviços de ativos virtuais (VASP) ou CASP no quadro europeu. A referida circunstância está prevista no artigo 13.º da Diretiva (UE) 2015/849, especialmente quando estes operam em jurisdições com supervisão limitada ou inexistente.

As moedas de privacidade intensificam as dificuldades associadas à atribuição das transações, ao reforçarem a pseudonimidade no que diz respeito à identidade. Tal gera uma limitação operacional essencial em termos de prova no processo penal, em particular no que se refere à ligação entre endereços e pessoas singulares ou coletivas concretas. As moedas de privacidade tornaram-se populares entre quem pretende passar despercebido. (Cremers et al., 2024).

A transferência de ativos entre diferentes *blockchains* é uma técnica conhecida como «pontes criptográficas», sendo este método ou ferramenta cada vez mais popular para o BC.

A utilização de pontes entre *blockchains*, de um ponto de vista jurídico, agrava a dimensão transnacional do BC, ao gerar problemas de competência jurisdicional e cooperação internacional, bem como uma limitação operacional adicional na reconstrução do percurso financeiro dos fundos.

5.4. ESPAÇOS CRIMINÓGENOS E FACILITADORES: MERCADOS DA *DARKNET*

Os mercados da *darknet* são sites ocultos na Internet, aos quais se acede através de software específico (como o Tor) e onde se paga com criptoativos anónimos. Esses mercados facilitam o comércio de bens e serviços ilegais e proporcionam aos branqueadores de capitais uma forma de converter fundos ilícitos em criptoativos e vice-

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

versa (Jordá et al., 2024). É extremamente complexo determinar com precisão a quantidade de fundos ilícitos que são branqueados através deste ativo virtual (Alessi Longa, 2025).

Na darknet, *o Silk Road* foi o mercado mais popular a funcionar na rede *Tor*, uma vez que permitia a comercialização anónima com criptoativos. Apesar de tentar manter o pseudonimato, o seu fundador, Ulbricht, foi detido pelo FBI em 2013 e acabou por ser condenado por várias acusações.

Tendo em conta a grande quantidade de fundos branqueados, afigura-se pertinente examinar o quadro jurídico existente com o objetivo de combater a lavagem de criptoativos por parte das organizações criminosas. Esses ambientes agravam os desafios estruturais à intervenção das autoridades e colocam desafios regulamentares e operacionais, tanto na obtenção de provas digitais como na identificação dos intervenientes, o que incide diretamente na eficácia da ação penal contra a BC. O caso ilustrou os desafios de regulamentar e monitorizar a *deep web* (Hemdani, 2025).

5.5. CONSIDERAÇÃO DOGMÁTICA FINAL

Todas estas técnicas revelam os limites do Direito Penal convencional para se adaptar a estruturas tecnológicas descentralizadas. Isto levanta questões sobre a delimitação da tipicidade e a eficácia das respostas normativas num ambiente digital em constante evolução.

6. QUADROS JURÍDICOS PARA COMBATER A LAVAGEM DE CRIPTOATIVOS POR PARTE DAS OC

Os quadros jurídicos relativos aos criptoativos estão altamente fragmentados a nível mundial, com alguns países a proibi-los por completo e outros a adotá-los integralmente. Tem-se procurado, através da Convenção das Nações Unidas contra o Crime Organizado Transnacional (UNTOC), combater o crime organizado transnacional.

6.1. CONVENÇÃO DAS NAÇÕES UNIDAS CONTRA A CRIMINALIDADE ORGANIZADA TRANSNACIONAL

A Convenção da UNTOC, de 2000, é o principal instrumento jurídico internacional para fazer face aos desafios da criminalidade organizada transnacional. Oferece um conjunto de instrumentos para que os Estados desenvolvam políticas e quadros jurídicos destinados a prevenir e combater as diferentes formas de criminalidade organizada, como a lavagem de dinheiro associada aos criptoativos (Kabra & Gori, 2025). Esta convenção é relevante, na medida em que esses ativos virtuais estão a assumir um papel cada vez mais importante no mundo financeiro das organizações criminosas. A UNTOC pode apoiar a perseguição e a prevenção da lavagem de criptoativos através do desenvolvimento de quadros jurídicos mais robustos, da cooperação internacional e da aplicação de normas comuns para combater as transações ilegais deste ativo virtual (Wang & Hsieh, 2023).

Nos seus artigos 1.º, 13.º, 16.º e 18.º, é regulamentada a cooperação transfronteiriça em matéria de assistência jurídica mútua, extradição e troca de informações. Uma vez que as transações com criptoativos podem envolver várias jurisdições, a ênfase da UNTOC

na cooperação internacional é essencial para localizar e levar à justiça os criminosos organizados que abusam deste ativo virtual. Por exemplo, a Agência Nacional contra o Crime (NCA) do Reino Unido desmantelou uma enorme rede de BC no valor de milhares de milhões de dólares, denominada Operação Desestabilizar (Anggriawan & Susila, 2024).

Esta rede servia uma vasta gama de OC, desde russos ricos e figuras influentes a nível global até cibercriminosos e traficantes de droga. A NCA identificou dois OC de língua russa, «Smart» e «TGR», como os mandantes. Até ao momento, a sua investigação resultou em 84 detenções e na apreensão de mais de 20 milhões de euros em dinheiro e criptoativos (UNODC2, 2024). Esta operação bem-sucedida foi possível graças ao trabalho conjunto dos signatários da convenção, entre os quais se encontram , a Polícia Metropolitana do Reino Unido, a *Direction Centrale de la Police Judiciaire* de França, o Gabinete de Controlo de Ativos Estrangeiros do Tesouro dos Estados Unidos, a Agência Antidrogas e o FBI. (FATF et al., 2025).

O artigo 34.º da UNTOC incentiva os Estados a adotarem medidas legislativas compatíveis para prevenir a BC, o que é fundamental para fazer face aos riscos crescentes de crimes financeiros relacionados com criptoativos. Por exemplo, o GAFI exige medidas de KYC e de diligência devida do cliente para identificar e comunicar transações suspeitas envolvendo criptoativos, as quais devem ser implementadas em todos os países, independentemente da sua legislação local. (FATF, 2024).

A UNTOC apoia o desenvolvimento de normas internacionais, ajudando os países a desenvolver capacidades otimizadas de cibersegurança e investigação para detetar crimes relacionados com criptoativos. UNODC. (2026) Por exemplo, os canais de partilha de informação da UNTOC apoiam as agências policiais da UE, como a Europol, no rastreio de transações ilegais envolvendo este ativo virtual. Neste contexto, pode envolver a Eurojust, a agência da UE para a cooperação judiciária, a fim de garantir uma perseguição transfronteiriça eficaz.

Neste contexto, a UNTOC oferece uma abordagem internacional com o objetivo de combater a lavagem de criptoativos, promovendo a cooperação internacional, a harmonização jurídica e o reforço de capacidades em matéria de aplicação da regulamentação.

6.2. RECOMENDAÇÕES DO GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL

O GAFI estabeleceu um conjunto abrangente de normas destinadas à mitigação e ao combate ao branqueamento de capitais e ao financiamento do terrorismo (BC/FT), que abrange os ativos virtuais e os prestadores de serviços de ativos virtuais (VASP). De uma perspetiva jurídica, o GAFI define «ativos virtuais» e «prestadores de serviços de ativos virtuais» para garantir a aplicação coerente e uniforme das suas normas. Os ativos virtuais são uma representação digital de valor que pode ser negociada ou transferida digitalmente e que pode ser utilizada para efetuar pagamentos ou investimentos (FATF, 2023).

Os VASP abrangem qualquer pessoa singular ou coletiva não abrangida noutro local pelas Recomendações e que, no âmbito da sua atividade comercial, se dedique a uma ou mais das seguintes atividades: a troca entre ativos virtuais e moedas fiduciárias; entre uma ou mais formas de outros ativos virtuais; a transferência de ativos virtuais; a custódia e/ou

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

gestão de ativos virtuais ou de instrumentos que permitam regular ativos virtuais; e a participação e prestação de serviços financeiros relacionados com a oferta e/ou venda de um ativo virtual por um emitente (FATF, 2021).

De uma perspetiva jurídica, a Recomendação 15 aborda especificamente os ativos virtuais, ao estabelecer que os países devem identificar e mitigar os riscos de branqueamento de capitais e financiamento do terrorismo (BC/FT) relacionados com ativos virtuais e VASP. O GAFI exige a aplicação da devida diligência em relação ao cliente (CDD), a manutenção de registos, a notificação de transações suspeitas (STR), os controlos internos e os programas de conformidade, bem como as sanções (FATF.1, 2023). Da mesma forma, a Recomendação 16 exige que os VASP obtenham, conservem e transmitam as informações do ordenante e do beneficiário nas transferências de ativos virtuais acima de um determinado limiar (1 000 USD/EUR). Por vezes, é designada por «regra de viagem».[7]

Esta norma visa prevenir a utilização de ativos virtuais para fins ilegais e garantir a transparência nas transações, na medida em que exige que os VASP partilhem estas informações com outras entidades obrigadas. A regra de viagem para ativos virtuais tem sido uma prioridade para o GAFI e continua a pressionar os países para que a implementem e a façam cumprir (Mollaahmetoğlu & Baykut, 2021).

O GAFI atualiza regularmente as suas recomendações sobre ativos virtuais para acompanhar os riscos em constante evolução e as inovações tecnológicas no mundo dos ativos virtuais. Os países devem incorporar estas regras na sua legislação e regulamentação nacionais. O GAFI continua a monitorizar a implementação destas normas em todo o mundo e insta as jurisdições a darem prioridade à sua implementação efetiva (Teng et al., 2026).

7. MODELOS REGULAMENTARES TRANSATLÂNTICOS FACE À LAVAGEM DE CAPITAIS COM CRIPTOATIVOS: AVALIAÇÃO COMPARATIVA EUA–UE

7.1. ESTADOS UNIDOS

Nos EUA não existe um quadro regulamentar unificado para os criptoativos; em vez disso, várias agências federais e estaduais supervisionam esses ativos virtuais. A *Securities and Exchange Commission*, ou Comissão de Valores Mobiliários dos EUA (SEC), regula os valores mobiliários e tem considerado muitos criptoativos e ofertas iniciais de moedas (ICO) como valores mobiliários. No processo SEC v. *Decentralized Autonomous Organization* (DAO), a SEC sustentou que os criptoativos são valores mobiliários e, por conseguinte, estão sujeitos à regulamentação da SEC (Lom & Hashmall, 2021). A *Commodity Futures Trading Commission* (CFTC), ou Agência Federal Independente dos EUA que regula os mercados de derivados, considera o bitcoin

[7] A Regra de Viagem é uma obrigação estabelecida pelo Grupo de Ação Financeira Internacional (GAFI/FATF) que exige que as entidades financeiras e os prestadores de serviços de ativos virtuais (VASPs) transmitam informações sobre o ordenante e o beneficiário juntamente com a transferência de fundos ou criptoativos. O seu objetivo é garantir a rastreabilidade e permitir que as autoridades identifiquem as partes envolvidas em transações que possam estar relacionadas com branqueamento de capitais, financiamento do terrorismo ou outros crimes graves.

e outros ativos virtuais como matérias-primas e regula os mercados de derivados e futuros sobre criptoativos (Hinojal, 2023).

A *Financial Crimes Enforcement Network*, ou Rede de Controlo/Execução de Crimes Financeiros (FinCEN), supervisiona as plataformas de câmbio de criptomoedas e os fornecedores de carteiras eletrónicas como transmissores de fundos, devendo estes cumprir os regulamentos PBC/FT e KYC. A *Internal Revenue* Service (IRS), ou Agência Federal de Recolha de Impostos dos Estados Unidos, trata os criptoativos como bens para efeitos fiscais, e os ganhos e perdas estão sujeitos ao imposto sobre mais-valias (Baer et al., 2023). A regulamentação tende a ser descentralizada; estados como Nova Iorque têm as suas próprias leis (*BitLicense*),[8] enquanto outros têm políticas mais flexíveis ou indefinidas.

A *BitLicense* é uma licença comercial que exige dos operadores regras mais rigorosas em matéria de combate à lavagem de dinheiro e ao financiamento do terrorismo (PBC/FT). Na Califórnia, a lei exige que os operadores de bitcoins mantenham reservas equivalentes às dos bancos para cobrir perdas, mas a Carolina do Norte ainda está a trabalhar em projetos de lei para a regulamentação das bitcoins e não possui qualquer diretiva em vigor (NYDFS, 2024–2026).

A Procuradoria-Geral dos EUA abriu um processo penal contra *Rule e Nysewander*[9] por conspiração com terceiros para branquear os lucros ilícitos provenientes de fraudes amorosas online, fraudes por e-mail empresarial, fraudes imobiliárias e outras fraudes através de criptoativos (Lim & Choi, 2025).

De acordo com a acusação da Procuradoria-Geral dos Estados Unidos, eles converteram os fundos ilícitos em criptoativos e transferiram-nos para contas controladas pelos seus cúmplices nos EUA e no estrangeiro. Isto evidencia uma estratégia destinada a ocultar a origem ilícita dos fundos e a dificultar a sua rastreabilidade. Além disso, ao abrirem contas e operarem com bancos e plataformas de *câmbio* de criptomoedas, *Rule e Nysewander* terão prestado declarações falsas e omitido informações relevantes com o objetivo de contornar os controlos e salvaguardas próprios destas instituições.

Como resultado destas ações, no âmbito desta alegada conspiração, eles e os seus cúmplices branquearam mais de 2,4 milhões de dólares americanos. Por fim, ambos foram declarados culpados e poderão enfrentar penas de até 20 anos de prisão federal por cada acusação de BC (Farrukh et al., 2025).

Da mesma forma, em agosto de 2024, Lam e Serrano foram acusados do roubo de criptoativos no valor de 230 milhões de dólares americanos (Trozze et al., 2022).

Os procuradores norte-americanos também têm vindo a investigar *a Binance*, a empresa que opera a maior plataforma mundial de câmbio de criptoativos, *a Binance.com*.

---

[8] A *BitLicense* é uma licença regulamentar obrigatória emitida pelo Departamento de Serviços Financeiros do Estado de Nova Iorque (NYDFS) para empresas que realizam atividades com criptomoedas ou ativos virtuais no estado de Nova Iorque ou com residentes de Nova Iorque. Foi introduzida em 2015 através do regulamento 23 NYCRR Parte 200.

[9] Trata-se de dois homens (de Nevada e da Carolina do Sul) que foram acusados e posteriormente condenados por participarem numa conspiração de branqueamento de capitais através de criptomoedas, segundo o Departamento de Justiça dos EUA.

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

A empresa declarou-se culpada e pagará mais de 4 000 milhões de dólares para resolver a investigação do Departamento de Justiça sobre violações da Lei de Sigilo Bancário (BSA), por não se ter registado como transmissor de fundos, e da Lei de Poderes Económicos de Emergência Internacional (IEEPA) (Departamento de Justiça dos EUA, 2023).

O canadiano Changpeng Zhao, fundador e ex-CEO da *Binance*, também se declarou culpado de não ter mantido um programa eficaz contra o branqueamento de capitais (PBC/FT ou AML), em violação da lei BSA. No âmbito do acordo de confissão de culpa, Zhao demitiu-se do cargo de CEO da Binance (Departamento de Justiça dos EUA.1, 2023).

Embora os procuradores norte-americanos tenham conseguido julgar com sucesso os lavadores de dinheiro e as plataformas de *câmbio* de criptomoedas, o mercado de criptoativos ainda requer maiores níveis de transparência, a fim de proteger os potenciais investidores (Anguren et al., 2023). Há algumas décadas, o boom do comércio eletrónico deu origem a quadros jurídicos de caráter inovador para esses ativos virtuais, e as suas múltiplas formas merecem uma orientação semelhante. A criação de regras claras para a venda de determinadas criptomoedas e fundos de criptomoedas poderia proporcionar a clareza tão necessária (Blanco Barón, 2025).

Sem um quadro regulamentar mais maduro, depender apenas das medidas coercivas de agências como a SEC não é suficiente para atingir os seus objetivos regulamentares. Em última análise, estas medidas punitivas podem prejudicar os próprios investidores que a SEC procura proteger e sufocar o investimento em empresas promissoras. Entre a regulamentação proposta para os criptoativos encontra-se o projeto de lei contra a lavagem de ativos digitais, que visa prevenir outros crimes relacionados com os ativos virtuais, mas colocando o foco naqueles que realizam as transações (mineradores, validadores, etc.) (Warren & Marshall, 2022).

O sistema norte-americano, de uma perspetiva jurídica, caracteriza-se por ser segmentado e reativo, uma vez que nele intervêm múltiplas agências com competências inter-relacionadas. A flexibilidade regulatória proporcionada por esta estrutura pode gerar problemas de coerência normativa e possíveis sobreposições de competências.

Esta abordagem apresenta limitações na prevenção *ex ante* no que diz respeito às moedas de base (BC), na medida em que a sua atuação se centra basicamente em mecanismos de *aplicação da lei* posteriores à prática do delito. A ausência de um quadro normativo unificado impede igualmente a aplicação uniforme das obrigações de conformidade por parte dos prestadores de serviços de ativos virtuais (VASP), o que, neste contexto, poderá gerar lacunas de risco regulatório.

7.2. UNIÃO EUROPEIA

Atualmente, a UE não dispõe de um quadro jurídico harmonizado para os criptoativos em todos os Estados-Membros. No entanto, a Comissão Europeia propôs algumas medidas, como a Sexta Diretiva contra o Branqueamento de Capitais (6AMLD), que exigiria que as empresas que trabalham com criptoativos se registassem junto das autoridades nacionais.

Cumprir as normas contra o branqueamento de capitais e comunicar qualquer transação suspeita. O objetivo da 6AMLD é colmatar as lacunas jurídicas das legislações nacionais dos países da UE através da criação de definições coerentes para o BC e os ativos virtuais em toda a UE (Parlamento Europeu, 2024).

Para estabelecer uma forma uniforme de regulamentar as transações com criptoativos em toda a UE, a Comissão Europeia recomendou o Regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos e a diretiva de alteração. Este conjunto de normas, denominado MiCA ([10]), tem como objetivo estabelecer uma estrutura de supervisão, que inclui normas para os emitentes, os prestadores de serviços e os participantes no mercado secundário.

Com base nestas regulamentações MiCA e 6AMLD, a 19 de setembro de 2024, a Polícia Criminal Federal Alemã desmantelou as infraestruturas de 47 plataformas de câmbio de criptomoedas em russo sem verificação de identidade (sem protocolo KYC). Esta operação, denominada «Operação Final Exchange», é de grande envergadura e evidencia o papel crucial que as plataformas de *câmbio* instantâneo sem KYC desempenham no cibercrime (Menacho-Inga et al., 2025). Tal como os seus nomes sugerem, esses sites sem protocolos KYC não dispõem de qualquer processo visível para recolher informações de identificação dos utilizadores antes de lhes permitirem depositar ou levantar qualquer montante. Não solicitam nomes, números de telefone nem endereços de e-mail e não se preocupam em verificar essas informações antes de realizar as transações (Anggriawan & Susila, 2024).

Uma das maiores vulnerabilidades do atual quadro regulamentar dos criptoativos é a ausência de uma autoridade central com capacidade para supervisionar e auditar as transações. Atribuir a supervisão e a regulamentação dos criptoativos a agências não especializadas reduz o impacto destas regulamentações. Além disso, no âmbito jurídico, não existem diretrizes nem requisitos prévios para a obtenção de licenças para operar no setor dos criptoativos (Hope Kanu, 2025).

Numa perspetiva comparativa, o modelo norte-americano apresenta uma abordagem fragmentada e reativa, baseada na intervenção a posteriori de diferentes agências. Por outro lado, o modelo da UE caracteriza-se por uma abordagem preventiva e harmonizada, orientada para diminuir a pseudonimidade *ex ante*. No entanto, ambos os sistemas têm, na sua capacidade operacional, limitações para fazer face à dimensão internacional do fenómeno.

Nenhum dos dois sistemas é totalmente eficaz. O modelo norte-americano pode apresentar lacunas na fase preventiva, enquanto o modelo europeu continua a enfrentar desafios na sua aplicação efetiva e na adaptação à rápida evolução tecnológica do ecossistema das criptomoedas.

8. NOVIDADES LEGISLATIVAS DA UNIÃO EUROPEIA

As estruturas societárias opacas utilizadas pelas organizações criminosas para branquear ativos virtuais, com entrada em vigor a 10 de julho de 2027, reforçarão a transparência da

[10] São as siglas de *Markets in Crypto-Assets Regulation*, o Regulamento (UE) n.º 2023/1114 relativo aos mercados de criptoativos. Trata-se da primeira regulamentação abrangente da UE que regula os criptoativos, os seus emitentes e os prestadores de serviços a eles associados.

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

titularidade real, ampliarão a rastreabilidade e o controlo sobre as operações com criptoativos, proibindo as contas anónimas (Regulamento (UE) 2024/1624, art. 79.1) e exigirá medidas específicas para as transferências para endereços auto-hospedados[11] (Regulamento (UE) 2024/1624, art. 40).

Ao mesmo tempo, o pacote normativo anterior foi revisto por uma nova diretiva sobre mecanismos de prevenção, que introduz a obrigação dos Estados-Membros de estabelecerem mecanismos para identificar a pessoa que detém ou controla contas de criptoativos e de interligar esses mecanismos através de um sistema a nível da UE (Diretiva (UE) 2024/1640, art. 16.º). De uma perspetiva jurídica, a supervisão europeia é reforçada com a criação da Autoridade AMLA, que está plenamente operacional desde 1 de julho de 2025 (Regulamento (UE) 2024/1620).

8.1. QUE ALTERAÇÕES INTRODUZ A UE EM RELAÇÃO AOS EUA PARA MITIGAR A PSEUDONIMIDADE E A OPACIDADE NA UTILIZAÇÃO DE CRIPTOATIVOS?

A UE proíbe os prestadores de serviços de criptoativos de manterem contas anónimas ou qualquer conta que permita ocultar o titular ou aumentar a opacidade das transações, referindo-se especificamente às moedas de privacidade (Regulamento (UE) 2024/1624, art. 79.º, n.º 1). Em consonância com esta abordagem, o pacote europeu PBC/FT estabelece a obrigação de os prestadores de serviços de criptoativos identificarem e avaliarem os riscos inerentes às transferências com endereços auto-hospedados. Da mesma forma, esses prestadores devem aplicar medidas de mitigação proporcionais, que podem incluir a identificação e verificação do remetente ou do destinatário e a recolha de informações adicionais sobre a origem e o destino (Regulamento (UE) 2024/1624, art. 40.1). Estas normas consolidam o objetivo de limitar a utilização de criptoativos para fins de anonimização, em particular quando combinados com estruturas societárias opacas — um contexto que o próprio quadro europeu reconhece como gerador de riscos de evasão e ofuscação e ao qual o novo pacote de 2024 dá resposta.

A UE optou por adotar o modelo de «tolerância zero» em relação à pseudonimização, com proibições diretas, regras uniformes e uma nova autoridade supranacional. Em contrapartida, os EUA seguem um modelo descentralizado, em que o anonimato não é proibido e as autoridades atuam principalmente através de ações penais ou administrativas após a deteção de infrações.

A grande diferença é simples. A UE limita a pseudonimização *ex ante* através de proibições e os EUA combatem-na *ex post* através *da aplicação da lei.*[12]

[11] Um endereço auto-hospedado é um endereço de criptomoeda controlado diretamente por um utilizador, sem intervenção nem custódia de um intermediário regulado (como uma bolsa ou um VASP).

[12] É um termo anglo-saxónico que se traduz como aplicação, execução ou cumprimento da lei. No âmbito jurídico e regulatório, descreve o conjunto de ações, medidas e procedimentos levados a cabo pelas autoridades competentes para garantir que as normas sejam efetivamente cumpridas. Em termos gerais: «*Enforcement*» é a capacidade e a prática de um Estado ou de uma autoridade reguladora para investigar, supervisionar, sancionar e corrigir incumprimentos normativos.

Tabela 1.
Principais diferenças entre a UE e os EUA em matéria de pseudonimidade e opacidade nos criptoativos.

DIMENSÃO	UE	EUA
Contas anónimas.	Explicitamente proibidas (art. 79.1).	Não proibidas pela legislação federal.
Moedas de privacidade	Proibição a partir de 2027.	Não são proibidas, mas estão sob vigilância.
Carteira de criptoativos auto-hospedada.	Avaliação obrigatória de riscos e possível identificação. (art. 40.1).	Não existe obrigação federal de identificação.
Quadro regulamentar.	Integral, unificado (MiCA + AMLR).	Fragmentado: SEC, CFTC, FinCEN, IRS, estados.
Supervisão.	Centralizada ao abrigo da AMLA.	Descentralizada; cada agência atua na sua área de competência.
Tokens privados.	Eliminação total.	Não proibidos.
Abordagem.	Preventivo, restritivo, rastreabilidade total.	Reativo, sancionatório, baseado na *aplicação da lei*.

8.2. QUE NOVIDADES AFETAM A IDENTIFICAÇÃO DO TITULAR REAL E A TRANSPARÊNCIA SOCIETÁRIA PERANTE ESTRUTURAS OPACAS?

O Regulamento (UE) 2024/1624 especifica a cadeia de identificação do titular efetivo por via da propriedade e do controlo, e que as informações sobre a titularidade efetiva sejam adequadas, precisas e atualizadas, e que as entidades informem o registo central sem demora injustificada e num prazo máximo de 28 dias consecutivos para comunicar qualquer alteração (Regulamento (UE) 2024/1624, art. 63). A informação necessária para obter dados sobre o titular efetivo é alargada e especificada, incluindo, entre outros, a identificação completa, a natureza e a extensão do interesse efetivo e, caso exista uma estrutura com múltiplas entidades ou instrumentos, a descrição da estrutura de propriedade e controlo (Regulamento (UE) 2024/1624, art. 62). De uma perspetiva jurídica, a Diretiva (UE) 2024/1640 estabelece normas relativas à criação e ao acesso a registos centrais de titularidade real e substitui a Diretiva (UE) 2015/849, que é revogada a partir de 10 de julho de 2027 (Diretiva (UE) 2024/1640; efeito revogatório).

Tudo isto em consonância com o reforço do quadro de transparência e cooperação em toda a UE, com o objetivo de limitar significativamente o recurso a empresas de fachada ou estruturas societárias opacas.

Em contrapartida, os Estados Unidos facilitam o recurso a estruturas societárias, dando uma reviravolta de 180º, reduzindo drasticamente a transparência, ao eliminar as obrigações para as empresas norte-americanas, enfraquecendo a *Lei de Transparência*

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

Corporativa (Corporate *Transparency Act)*[13] e deixando a transparência a cargo dos estados.

Tabela 2.

Comparação do quadro de transparência da titularidade real e da supervisão em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo: União Europeia vs. Estados Unidos.

ELEMENTO	UNIÃO EUROPEIA	ESTADOS UNIDOS
Cadeia de identificação do titular efetivo.	Detalhada, alargada e obrigatória (propriedade + controlo, extensão da participação, estrutura societária completa).	Eliminada quase na totalidade para entidades nacionais a partir de 2025; aplica-se apenas a algumas entidades estrangeiras.[14]
Atualização de dados.	Prazo máximo de 28 dias corridos para notificar alterações.	Não existe qualquer obrigação a nível federal para as empresas norte-americanas.
Registos centrais.	Obrigatoriedade e harmonização ao abrigo da Diretiva 2024/1640.	Não existe registo federal para entidades nacionais após a IFR de 2025; a transparência depende dos estados. [15]
Estratégia face às empresas de fachada.	Restritiva, preventiva e baseada na rastreabilidade integral.	Flexibilização regulamentar: o fim do sistema de comunicação federal facilita a utilização de estruturas societárias opacas.
Supervisão AML PBC/FT.	Modelo europeu unificado com a AMLA.	*Aplicação* fragmentada (FinCEN, IRS, SEC, CFTC), sem uma estrutura federal única para os beneficiários efetivos.

[13] A *Corporate Transparency Act* (CTA) é uma lei federal dos Estados Unidos, promulgada em 2021, cujo objetivo é combater a lavagem de capitais, o financiamento do terrorismo, a fraude fiscal e a utilização de sociedades de fachada, através da obrigação de comunicar informações sobre os beneficiários efetivos (*Beneficial Ownership Information*, BOI) de determinadas entidades.

[14] Financial Crimes Enforcement Network. (2025). *Beneficial Ownership Information Reporting. Departamento do Tesouro dos EUA*. 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). *Atualização da CTA: Uma análise do estado dos requisitos de comunicação de titularidade efetiva ao abrigo da Lei de Transparência Empresarial e iniciativas relacionadas, a 5 de janeiro de 2026.* Pillsbury Winthrop Shaw Pittman LLP. https://www.pillsburylaw.com/en/news-and-insights/cta-update.html

8.3 IMPLICAÇÕES JURÍDICO-DOGMÁTICAS DA IDENTIFICAÇÃO DO TITULAR REAL

Do ponto de vista dogmático, o Regulamento (UE) n.º 2024/1624 não constitui um mero reforço da transparência formal, na medida em que incide diretamente no desenvolvimento estrutural do conceito de titularidade real. Com isso, consegue-se deslocar a prioridade de uma perspetiva meramente registal para um princípio material baseado na supervisão efetiva.

Do ponto de vista do Direito Penal Económico, esta mudança é bastante relevante, uma vez que reduz as margens de imputação indefinida que são próprias das organizações societárias complexas. Quando se solicita a identificação do titular real tendo em conta tanto a propriedade como a supervisão, o Regulamento estabelece um critério funcional que simplifica a atribuição jurídica de responsabilidade. É especialmente em crimes de BC que a ocultação do beneficiário final constitui um elemento típico central.

Neste mesmo sentido, a exigência de que a informação sobre a titularidade real seja adequada, exata e atualizada, juntamente com a obrigação de notificação num prazo máximo de 28 dias (art. 63.º), não tem apenas um aspeto administrativo, mas também produz efeitos diretos sobre a eficácia probatória no processo penal. Nesse sentido, os registos de titularidade real afirmam-se como verdadeiros instrumentos de análise do *iter criminis* financeiro. Esta situação contribui para limitar o risco na fase de investigação e para facilitar a rastreabilidade jurídica dos fundos ilícitos.

O alargamento do conteúdo informativo (art. 62.º), que inclui a natureza e a extensão do interesse real e a análise de estruturas complexas, introduz, por seu lado, um aspeto fundamental na dogmática do branqueamento de capitais. Tal permite estabelecer uma relação jurídica entre a titularidade económica e a aparência formal de legalidade. Esta relação é essencial para contornar os limites convencionais do Direito Penal face a aspetos de estratificação e segregação patrimonial, elementos comuns do branqueamento de capitais através de criptoativos.

Em conformidade com esta abordagem, a Diretiva (UE) 2024/1640 reforça a configuração dos sistemas de acesso e centralização da informação. Desta forma, estabelece-se uma perspetiva que vai além da simples harmonização normativa, passando para um quadro jurídico de transparência a nível supranacional. Este desenvolvimento implica uma otimização do princípio da cooperação administrativa e judicial na UE, princípio essencial num contexto de criminalidade transnacional.

Podemos afirmar que, no seu conjunto, estas normas criam as condições para sustentar o modelo europeu, ao regerem-se por uma lógica preventivo-estrutural, orientada não apenas para sancionar condutas, mas também para limitar *ex ante* as condições de possibilidade do crime, restringindo a utilização de instrumentos societários como mecanismos de opacidade.

O modelo dos EUA, pelo contrário, tem implicações significativas para a teoria do Direito. Enfraquecer a *Corporate Transparency Act* e atenuar as obrigações de identificação do titular efetivo implica uma mudança para um sistema em que, consequentemente, a opacidade societária volta a ser uma área de risco jurídico relevante.

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

Do ponto de vista dogmático, isto complica a identificação do sujeito ativo do crime e dificulta a imputação penal em estruturas complexas.

Esta postura põe em evidência uma disparidade estrutural entre ambos os sistemas. Por um lado, a UE desenvolve um modelo baseado na identificação *ex ante* e na rastreabilidade jurídica. Por outro lado, os EUA mantêm uma lógica maioritariamente reativa, baseada na *aplicação da lei*, em que a intervenção ocorre após a prática do ilícito.

De um ponto de vista crítico, esta divergência não é apenas técnica, mas reflete duas conceções distintas do Direito Penal Económico:

Um modelo europeu de prevenção estrutural e redução do risco sistémico.

Um modelo norte-americano de reação punitiva, de perseguição do crime.

Na verdade, o desenvolvimento normativo europeu evidencia um esforço para resolver a disparidade convencional entre rastreabilidade económica e imputação jurídica. Em contrapartida, o modelo norte-americano continua a apresentar dificuldades para integrar ambos os planos de forma coerente no âmbito da BC.

8.4. COMO SÃO REFORÇADOS OS MECANISMOS DE LOCALIZAÇÃO DE CONTAS E A SUPERVISÃO EUROPEIA PARA DETETAR ESQUEMAS ENVOLVENDO CRIPTOATIVOS E EMPRESAS COM ESTRUTURAS OPACAS?

A Diretiva (UE) 2024/1640 exige que os Estados-Membros estabeleçam mecanismos automatizados centralizados que permitam identificar em tempo real qualquer pessoa que seja titular ou controle, entre outros produtos, contas de criptoativos, bem como contas bancárias, contas de pagamento, contas de valores mobiliários e cofres (Diretiva (UE) 2024/1640, art. 16.º, n.º 1).

Esses mecanismos devem incluir informações mínimas sobre o titular, o representante, o beneficiário efetivo e as datas de abertura e encerramento; no caso das contas de criptoativos, devem incluir ainda um identificador único e as datas de abertura e encerramento (Diretiva (UE) 2024/1640, art. 16.3.f). Da mesma forma, deve estar prevista a sua interligação através do sistema BARIS[16] , que a Comissão deve criar e gerir, com o objetivo de concretizar a interligação o mais tardar em 10 de julho de 2029 (Diretiva (UE) 2024/1640, art. 16.º, n.º 6).

Este reforço é complementado com a criação da AMLA[17] para supervisionar e unificar a supervisão, bem como para tornar mais eficaz o sistema europeu na prevenção

[16] *O Sistema de Interligação de Registos de Contas Bancárias* (BARIS) é um sistema informático de âmbito europeu concebido para interligar os registos nacionais de contas bancárias dos Estados-Membros da UE, permitindo um acesso rápido, seguro e harmonizado à informação financeira relevante para a prevenção, deteção, investigação e repressão de crimes graves, incluindo o branqueamento de capitais e o financiamento do terrorismo.

[17] A AMLA (*Anti-Money Laundering Authority* / Autoridade Europeia de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo) é uma agência descentralizada da UE, criada em 2024 e com sede em Frankfurt, cujo objetivo é supervisionar, coordenar e reforçar o cumprimento das normas europeias em matéria de prevenção da lavagem de dinheiro (AML) e do financiamento do terrorismo (CFT).

dos riscos transfronteiriços de branqueamento de capitais e financiamento do terrorismo (Regulamento (UE) 2024/1620; entrada em vigor geral a 1 de julho de 2025), no âmbito do pacote legislativo europeu de 2024.

9. EFICÁCIA DO QUADRO REGULAMENTAR NA LUTA CONTRA A LAVAGEM DE CAPITAIS ATRAVÉS DE CRIPTOATIVOS

A capacidade de prevenir, detetar, atribuir a autoria e sancionar a lavagem de capitais, vista numa perspetiva de eficácia regulatória, exige uma análise comparativa desses quadros, na medida em que deve ser considerada também em relação aos princípios da legalidade e da segurança jurídica. A determinação dos comportamentos típicos e a sua investigação eficaz dependem da precisão normativa e da capacidade de adaptação do direito penal económico em ambientes tecnológicos sofisticados.

A análise da eficácia dos quadros regulamentares em matéria de BC por meio de criptoativos deve ir além de uma abordagem formal centrada na existência de normas. O seu objetivo é avaliar a sua capacidade real de prevenir, detetar e perseguir as condutas ilícitas num ambiente tecnologicamente sofisticado, bem como a dimensão internacional deste fenómeno. O grau de desenvolvimento normativo deve também ser examinado com base na sua operacionalidade prática e na sua capacidade de adaptação às dinâmicas do ecossistema das criptomoedas.

É possível identificar critérios jurídicos e operacionais a partir desta premissa, para avaliar a eficácia dos sistemas de PBC neste domínio.

9.1. CAPACIDADE DE PREVENÇÃO

Para que um sistema seja eficaz nas políticas de prevenção e repressão contra a BC, o primeiro pilar é a prevenção. Este primeiro pilar concretiza-se principalmente no âmbito dos criptoativos, nas obrigações de diligência devida previstas no artigo 13.º da Diretiva (UE) 2015/849, de conhecimento do cliente (KYC) e de avaliação do risco que os VASP devem cumprir.

O modelo da UE apresenta uma abordagem mais sólida, um sistema harmonizado com obrigações definidas para os intermediários, reforçando a rastreabilidade e restringindo a pseudonimidade. O modelo norte-americano, pelo contrário, depara-se com inúmeras limitações operacionais para estabelecer obrigações uniformes, o que poderá dar origem a lacunas de risco.

No entanto, a eficácia preventiva não depende apenas da existência destas obrigações, mas também de uma aplicação e supervisão adequadas.

9.2. CAPACIDADE DE DETECÇÃO

A deteção de operações suspeitas é crucial para mitigar o BC. No âmbito das moedas digitais, essa capacidade traduz-se na utilização de instrumentos de análise de *blockchain* e na colaboração entre atores públicos e privados.

A rastreabilidade ou acompanhamento técnico destas operações em redes públicas permite que tal não implique, nem sempre, uma identificação efetiva dos participantes

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

envolvidos. A eficácia das normas regulamentares reside na incorporação de capacidades técnicas pelas autoridades e na colaboração com organismos especializados.

9.3. CAPACIDADE DE ATRIBUIÇÃO

Tal como referido na análise da titularidade real, o reforço dos sistemas de identificação previstos no Regulamento (UE) n.º 2024/1624 contribui para colmatar a clássica lacuna entre a rastreabilidade técnica e a atribuição jurídica. No BC através de criptoativos, um dos principais desafios estruturais que se coloca reside na separação entre a rastreabilidade das transações e a atribuição jurídica a pessoas singulares ou coletivas específicas.

Desta forma, a exigência de informações precisas, atualizadas e funcionalmente completas sobre o beneficiário efetivo permite identificar pontos de ligação entre as transações registadas em sistemas descentralizados. Um exemplo disso é , a *blockchain* e determinadas entidades jurídicas, uma vez que facilitam assim a imputação penal nos casos de BC.

Do ponto de vista dogmático, esses mecanismos reforçam a possibilidade de identificar o verdadeiro titular económico para além das construções formais, o que se reveste de importância essencial para a constituição do elemento subjetivo do crime e para a comprovação do conhecimento sobre a origem ilícita dos fundos. Desta forma, a arquitetura normativa europeia não só reforça a capacidade de deteção, como também incide de forma decisiva na capacidade de atribuição jurídica, superando uma das principais lacunas estruturais do sistema tradicional face às novas formas de criminalidade financeira baseadas em criptoativos.

É necessário provar a existência de operações suspeitas para que se investigue um crime, a sua relação com um determinado sujeito e o conhecimento da origem ilícita dos fundos. As redes *blockchain*, juntamente com a utilização de *mixers*, moedas de privacidade ou estruturas de estratificação, dificultam esta tarefa devido à sua natureza pseudónima.

A eficácia dos quadros regulamentares depende da sua capacidade de criar pontos de ligação entre o domínio digital e o mundo jurídico, através de mecanismos de identificação e obrigações de informação.

9.4. CAPACIDADE DE EXECUÇÃO E SANÇÃO

O último elemento de avaliação consiste na capacidade de investigar, sancionar e apreender os ativos ilícitos. Esta dimensão apresenta características próprias no âmbito dos criptoativos, tais como *a blockchain*, as transferências transfronteiriças e as limitações operacionais e técnicas à sua apreensão.

A abordagem baseada na *aplicação da lei*, em conformidade com o modelo norte-americano, caracteriza-se por uma forte capacidade de investigação e ação penal. Este caráter reativo, no entanto, pode não ser suficiente se não for complementado com medidas preventivas.

Em contrapartida, observamos um reforço da UE nos seus instrumentos de supervisão através da criação da AMLA, cuja eficácia depende da sua capacidade de coordenar as autoridades nacionais.

9.5. AVALIAÇÃO COMPARATIVA DA EFICÁCIA

Este critério revela-nos, após análise, que nenhum dos modelos, por si só, se revela plenamente eficaz. O sistema norte-americano apresenta pontos fortes na aplicação de sanções, mas deficiências na prevenção estrutural. No entanto, o modelo da UE proporciona um quadro mais coerente e preventivo, embora enfrente um desafio estrutural na sua aplicação.

Para que os quadros regulamentares sejam eficazes, não apenas através do desenvolvimento normativo, é necessário que haja interação entre a regulamentação, as capacidades tecnológicas, a cooperação internacional e a especialização institucional. A separação entre planeamento normativo e a capacidade operacional constitui o principal problema, o que reforça a necessidade de uma abordagem integral e coordenada.

A necessidade de uma evolução do Direito Penal Económico põe em evidência que é possível conciliar a eficácia na investigação com o respeito pelas garantias fundamentais.

10. CONCLUSÕES

A análise desenvolvida ao longo deste trabalho permite confirmar que a eficácia dos quadros regulamentares em matéria de BC através de criptoativos não depende apenas do seu grau de desenvolvimento normativo. Neste sentido, depende da sua capacidade real para prevenir, detetar, atribuir a responsabilidade e sancionar condutas ilícitas, ao criar as condições para afirmar que os criptoativos, as criptomoedas e os ativos virtuais dão origem a métodos singulares, graças ao seu pseudonimato e à natureza global e descentralizada da tecnologia *blockchain*, um fenómeno em expansão. As organizações criminosas exploram estas características propositadamente, utilizando uma combinação de ofuscação sofisticada (por exemplo, *smurfing*, carteiras de criptoativos, serviços de mistura, moedas privadas, pontes entre *blockchains*) e estruturas corporativas opacas.[18] Com isso, consegue-se fragmentar, deslocar e ocultar o rasto do fundo, das transações e dos serviços de mistura, das moedas privadas e das pontes — veículos suscetíveis de exploração ilícita para conferir maior opacidade aos seus rastros. Esta combinação tecnológica e societária evidencia que a utilização ilícita desses ambientes não é acidental, mas sim estratégica e deliberada. Os mercados da *darknet*, no entanto, atuam como facilitadores nesses casos, oferecendo, por conseguinte, espaços para o comércio anónimo.

Com base na análise realizada, pode afirmar-se que o BC, através dos criptoativos, é um fenómeno complexo. Caracteriza-se pela interação entre a infraestrutura tecnológica do ecossistema digital, a dimensão internacional das operações e a capacidade de

[18] Uma sociedade opaca é uma entidade jurídica cuja estrutura de propriedade, controlo e beneficiários efetivos foi concebida para ocultar a identidade das pessoas que realmente detêm ou controlam a empresa. A sua característica essencial é a falta de transparência, que impede a identificação do titular efetivo (*ultimate beneficial owner*, UBO).

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

adaptação das OC. A existência de quadros normativos neste sentido não é suficiente para garantir a sua eficácia.

Os EUA e a UE apresentam abordagens muito diferenciadas no que diz respeito aos seus modelos regulamentares. Enquanto o modelo norte-americano se baseia numa abordagem centrada na *aplicação da lei,* na capacidade de investigação e na imposição de sanções, a UE, por seu lado, desenvolveu um sistema mais harmonizado e preventivo, orientado para limitar a pseudonimidade e reforçar a rastreabilidade das transações. Ambos os modelos, quer na prevenção estrutural, quer na aplicação concreta das normas, apresentam limitações evidentes.

A rastreabilidade técnica das transações, como já foi referido, nem sempre se traduz numa identificação efetiva dos sujeitos envolvidos, o que gera desafios probatórios essenciais e limita a imputação jurídica do crime. Por isso, a eficácia do quadro regulamentar não pode ser medida apenas pelo grau de desenvolvimento normativo. Deve ser avali e a partir da capacidade real de prevenção, deteção, imputação e sanção das condutas ilícitas.

A ideia de que a eficácia depende da integração de mecanismos de supervisão, capacidades técnicas e cooperação internacional corrobora esta realidade. A utilização de carteiras de criptoativos de terceiros, serviços de *«mixing»*, moedas de privacidade ou mercados na *darknet e na deep web* evidencia que a problemática não reside apenas no pseudonimato, mas na combinação de fatores tecnológicos, regulamentares e institucionais.

O esforço institucional para a mitigação da BC através de criptoativos requer uma abordagem integral que combine regulamentação, tecnologia e capacidade operacional, colmatando a lacuna entre a conceção normativa e a sua aplicação efetiva. Através desta interação, facilita-se o reforço da prevenção, deteção e repressão no âmbito dos criptoativos, na medida em que nenhum dos modelos analisados se revela plenamente eficaz por si só.

A principal contribuição deste estudo consiste em ter identificado a desconexão entre a rastreabilidade tecnológica e a atribuição jurídica como eixo central das limitações atuais do sistema de prevenção do BC em criptoativos.

11. REFLEXÃO FINAL

O estudo do BC através dos criptoativos põe em evidência um fenómeno que vai além das categorias tradicionais do direito penal e da regulamentação financeira. A evolução tecnológica trouxe consigo, não só possibilidades de inovação e novas formas de circulação de valor, como também abriu possibilidades de gerar espaços de risco, com a dificuldade de os enquadrar nos modelos normativos existentes.

Este estudo comparativo evidencia que nem uma abordagem centrada na *aplicação* da *lei*, nem um modelo predominantemente preventivo são suficientes por si sós, uma vez que se torna necessário repensar os mecanismos convencionais de intervenção jurídica. A capacidade dos sistemas jurídicos para se adaptarem a um ambiente marcado pela velocidade, pela descentralização e pela complexidade técnica constitui o novo desafio

que somos obrigados a enfrentar, bem como a necessidade de regulamentações mais modernas.

No contexto dos criptoativos, que refletem uma tensão crescente entre rastreabilidade técnica e atribuição jurídica, entre regulamentação formal e eficácia operacional, o BC vai além das divergências entre jurisdições. O novo papel das instituições obriga a repensar a tensão surgida, a cooperação internacional e a integração de capacidades tecnológicas como elementos essenciais do sistema.

A resposta institucional definitiva para mitigar este fenómeno não pode ser apenas normativa, mas também tecnológica. Com uma abordagem integral, será possível reduzir a distância entre o desenvolvimento das normas e a sua implementação eficiente, garantindo uma resposta jurídica coerente face a um fenómeno em constante evolução.

12. REFERÊNCIAS BIBLIOGRÁFICAS

Anggriawan, R., & Susila, M. (2024). A criptomoeda e a sua ligação com o branqueamento de capitais e o financiamento do terrorismo no âmbito das recomendações do FATF. *Novum Jus, 18(2)*. Disponível em: https://doi.org/10.14718/novumjus.2024.18.2.10 [Última consulta: 23/02/2026].

Akkoyun, A. G., & Çelik, M. E. (2022). Crime organizado transnacional e a Convenção da ONU. *Frontiers in Law, 1, 9–21*. Disponível em: https://doi.org/10.6000/2817-2302.2022.01.02 [Última consulta: 23/02/2026].

Alessi Longa, F. (2025). Criptomoedas e branqueamento de capitais. *American Journal of Industrial and Business Management, 15(2), 362–371*. Disponível em: 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). A regulamentação dos criptoativos no contexto internacional e europeu atual. *Revista de Estabilidade Financeira*, 44, Banco de Espanha. Disponível em: https://doi.org/10.53479/30054 [Última consulta: 23/02/2026].

Arnone, G., Scirè, G., & Bivona, E. (2025). O (mau) uso das criptomoedas por organizações criminosas: uma revisão sistemática da literatura. *Digital Finance, 7, 815–851*. Disponível em: 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). Análise forense da blockchain: uma revisão sistemática da literatura. *Electronics, 13(17), 3568*. Disponível em: https://doi.org/10.3390/electronics13173568 [Última consulta: 23/02/2026].

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

Béres, F., Seres, I. A., Benczúr, A. A., & Quintyne-Collins, M. (2021). A blockchain está a observar-te: criação de perfis e desanonimização de utilizadores da Ethereum. *Conferência Internacional IEEE de 2021 sobre Aplicações e Infraestruturas Descentralizadas (DAPPS), 69–78*. Disponível em: 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). Um estudo sobre a tecnologia blockchain: evolução, arquitetura e segurança. *IEEE Access, 9, 61048–61073*. Disponível em: https://doi.org/10.1109/ACCESS.2021.3072849 [Última consulta: 23/02/2026].

Blanco Barón, C. (2025). A regulamentação dos criptoativos: para além de um problema de eficiência. *Revista de Economia Institucional, 27(53), 133–186*. Disponível em: https://doi.org/10.18601/01245996.v27n53.07 [Última consulta: 23/02/2026].

Chiang, S. (2024). As criptomoedas estão a ser cada vez mais utilizadas para a lavagem de dinheiro. CNBC. Disponível em: https://www.cnbc.com/2024/07/16/crypto-is-increasingly-being-used-for-money-laundering-chainalysis-says.html [Último acesso: 23/02/2026].

Cremers, C., Loss, J., & Wagner, B. (2024). Uma análise holística da segurança das transações Monero. Em Advances in Cryptology – EUROCRYPT 2024 (pp. 129–159). *Springer*. Disponível em: https://doi.org/10.1007/978-3-031-58734-4_5 [Última consulta: 23/02/2026].

Enríquez Pérez, I. (2020). O crime organizado e a fragilidade institucional como fatores condicionantes do desenvolvimento. *Revista da Faculdade de Ciências Económicas*, 28(1). Disponível em: https://doi.org/10.18359/rfce.3564 [Último acesso: 23/02/2026].

Farrukh, H., Zafar, S., Rehman, Z. U., Shah, A. A., & Alshammry, N. (2025). Detecção de fraudes com base em blockchain: uma revisão sistemática comparativa da literatura sobre abordagens de aprendizagem federada e de aprendizagem automática. *Electronics*, 14(24), 4952. Disponível em: https://doi.org/10.3390/electronics14244952 [Última consulta: 23/02/2026].

Fu, Q., Liu, J., Pan, S., & Yuen, T. H. (2025). SoK: Uma análise aprofundada das técnicas de combate ao branqueamento de capitais para criptomoedas em blockchain. *Em ACISP 2025*. Disponível em: https://doi.org/10.1007/978-981-96-9095-4_16 [Último acesso: 23/02/2026].

Gorjón, S. (2023). As finanças descentralizadas ou os criptoativos de última geração. *Boletim Económico 2023/T3*, art. 04. Disponível em: 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». Em *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (pp. 217–247). *Springer*. Disponível em: https://doi.org/10.1007/978-3-031-80557-8_10 [Última consulta: 23/02/2026].

Hinojal, A. (2023). Criptomoedas e branqueamento de capitais. *Logos Guardia Civil, 1, 215–240*. Disponível em: revistacugc.es/article/view/5742 [Último acesso: 23/02/2026].

Holt, T. J., Lee, J. R., & Griffith, E. (2023). Uma avaliação dos serviços de «cryptomixing» nos mercados ilícitos online. *Journal of Contemporary Criminal*

Justice. Disponível em: https://doi.org/10.1177/10439862231158004 [Último acesso: 23/02/2026].

Hope Kanu, D. (2025). Regulamentação das criptomoedas e as suas implicações para a estabilidade financeira: uma análise qualitativa. *IJEBMR, 9(4)*. Disponível em: https://doi.org/10.51505/IJEBMR.2025.9416 [Última consulta: 23/02/2026].

Isolauri, E. A., & Ameer, I. (2023). A lavagem de dinheiro como fenómeno empresarial transnacional: uma revisão sistemática e agenda futura. *Critical Perspectives on International Business, 19(3), 426–468*. Disponível em: https://doi.org/10.1108/cpoib-10-2021-0088 [Última consulta: 23/02/2026].

Jordá, C., Píriz, C., & Giménez-Salinas, A. (2024). Os mercados ilícitos de tráfico de drogas na Dark Web: um estudo exploratório empírico. *Revista Espanhola de Investigação Criminológica, 22(2)*. Disponível em: https://doi.org/10.46381/reic.v22i2.884 [Última consulta: 23/02/2026].

Kabra, S., & Gori, S. (2025). Combate à lavagem de criptomoedas por grupos do crime organizado através de um quadro regulamentar eficaz. *IIUM Law Journal, 33(1)*. Disponível em: 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). Modelização de padrões de «smurfing» em criptomoedas com partições de números inteiros. *IET Blockchain*. Disponível em: https://doi.org/10.1049/blc2.12087 [Última consulta: 23/02/2026].

Langdale, J. (2024). Combate à lavagem de dinheiro em casinos do Sudeste Asiático e da Austrália. Em Financial Crime and the Law (pp. 225–245). *Springer*. Disponível em: https://doi.org/10.1007/978-3-031-59543-1_9 [Último acesso: 23/02/2026].

Legrand, T., & Leuprecht, C. (2021). Garantir a colaboração transfronteiriça: redes transgovernamentais de aplicação da lei. *Policy and Society*, 40(4), 565–586. Disponível em: https://doi.org/10.1080/14494035.2021.1975216 [Última consulta: 23/02/2026].

Lim, A., & Choi, K.-S. (2025). Modus operandi e análise de blockchain de golpes românticos: vitimização impulsionada por criptomoedas. *International Journal of Cybersecurity Intelligence & Cybercrime, 8(2)*. Disponível em: https://doi.org/10.52306/2578-3289.1220 [Última consulta: 23/02/2026].

Lom, A., & Hashmall, R. (2021). *Novas orientações da FATF sobre ativos virtuais e VASPs*. Disponível em: https://www.nortonrosefulbright.com/en-us/knowledge/publications/024b3d80/new-fatf-guidance-released-on-virtual-assets-and-virtual-asset-service-providers [Último acesso: 23/02/2026].

Luna Galván, M., Luong, H. T., & Astolfi, E. (2021). O tráfico de droga como crime organizado: uma perspetiva transnacional e multidimensional. *Revista de Relações Internacionais, Estratégia e Segurança, 16(1)*. Disponível em: https://doi.org/10.18359/ries.5412 [Última consulta: 23/02/2026].

Medranda Morales, N., & Arcos Argudo, M. (2023). Criptoativos e criptomoedas. Em Blockchain, criptoativos e metaverso (pp. 41–62). *Editora Abya-Yala*. Disponível em: https://doi.org/10.17163/abyaups.6 [Último acesso: 23/02/2026].

Menacho-Inga, W. G., Proaño-Reyes, G., & Castro-Sánchez, F. (2025). A utilização de criptomoedas e o branqueamento de capitais no Equador. *Noesis, 7(esp2)*. Disponível em: https://doi.org/10.35381/noesisin.v7i2.620 [Última consulta: 23/02/2026].

Mollaahmetoğlu, M. B., & Baykut, C. (2021). *Orientações atualizadas do Grupo de Ação Financeira Internacional (GAFI)*. Disponível em: https://chambers.com/articles/financial-action-task-force-s-updated-guidance-virtual-assets-and-virtual-asset-service-providers [Último acesso: 23/02/2026].

Montoya Arrubla, E. (2025). *Mecanismos de controlo da lavagem de criptoativos*. Diálogos Punitivos. Disponível em: https://dialogospunitivos.com/wp-content/uploads/2025/04/Columna-de-interes-43.pdf [Última consulta: 23/02/2026].

Rodríguez-Valencia, L., et al. (2025). Uma revisão sistemática da inteligência artificial aplicada à conformidade: deteção de fraudes em transações com criptomoedas. *Journal of Risk and Financial Management, 18(11), 612*. Disponível em: https://doi.org/10.3390/jrfm18110612 [Última consulta: 23/02/2026].

Soltani, R., Zaman, M., Joshi, R., & Sampalli, S. (2022). Tecnologias de registo distribuído e as suas aplicações: uma revisão. *Applied Sciences, 12(15), 7898*. Disponível em: https://doi.org/10.3390/app12157898 [Último acesso: 23/02/2026].

Sudan, H. K., Tai, A. M. Y., Kim, J., & Krausz, R. (2023). Desvendando os mercados de criptomoedas. Drug Science, *Policy and Law, 9, 1–19*. Disponível em: 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). Ativos digitais: riscos, regulamentação e mitigação. *Financial Innovation, 12, 65*. Disponível em: https://doi.org/10.1186/s40854-025-00848-y [Último acesso: 23/02/2026].

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Criptomoedas e a criminalidade financeira no futuro. *Crime Science, 11(1)*. Disponível em: https://doi.org/10.1186/s40163-021-00163-8 [Última consulta: 23/02/2026].

Wang, H.-M., & Hsieh, M.-L. (2023). As criptomoedas estão na moda: uma reflexão sobre a prevenção do branqueamento de capitais. *Security Journal*, *37, 25–46*. Disponível em: https://doi.org/10.1057/s41284-023-00366-5 [Última consulta: 23/02/2026].

Warren, E., & Marshall, R. (2022). *Lei contra a Lavagem de Dinheiro de Ativos Digitais de 2022 (S.5267)*. Senado dos Estados Unidos. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/5267 [Última consulta: 23/02/2026].

13. RELATÓRIOS DE ORGANISMOS

AMLC. (2023). *Análise de transações suspeitas associadas a junkets de casino*. Disponível em: 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). *Avaliação Nacional da Ameaça das Drogas 2025*. Disponível em: https://www.dea.gov/documents/2025/2025-05/2025-05-13/national-drug-threat-assessment [Última consulta: 23/02/2026].

Europol. (2024). *Criptomoedas – Rastrear a evolução das finanças criminosas*. Disponível em: 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). Criptomoedas: Traçando a evolução das finanças criminosas. *Série Europol Spotlight*. Disponível em: https://doi.org/10.2813/75468 [Última consulta: 23/02/2026].

FATF, Grupo Egmont, INTERPOL e UNODC. (2025). *Cooperação internacional na deteção, investigação e ação penal em matéria de branqueamento de capitais: Manual*. Paris: FATF. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html [Última consulta: 23/02/2026].

FATF. (2024). *Ativos virtuais: normas da FATF e implementação*. FATF. Disponível em: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Última consulta: 23/02/2026].

FATF. (2023). *Atualização específica sobre a implementação das normas da FATF relativas aos ativos virtuais e aos prestadores de serviços de ativos virtuais (VASPs)*. FATF. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [Última consulta: 23/02/2026].

FATF.1. (2023). *Ativos virtuais:* Normas *globais* da FATF. Disponível em: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Última consulta: 23/02/2026].

FATF. (2022). *Branqueamento de capitais proveniente do fentanil e dos opiáceos sintéticos*. Disponível em: 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). *Orientações atualizadas para uma abordagem baseada no risco em relação aos ativos virtuais e aos VASPs*. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf [Última consulta: 23/02/2026].

FinCEN. (2025). *Aviso sobre redes chinesas de branqueamento de capitais.* Disponível em: https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering [Última consulta: 23/02/2026].

Ministério do Interior. (2024, 15 de novembro). *Operação conjunta da Polícia Nacional e da Nationale Politie dos Países Baixos (método OTC).* Disponível em: https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16371# [Última consulta: 23/02/2026].

NYDFS. Departamento de Serviços Financeiros do Estado de Nova Iorque. (2024–2026). *Licenciamento de Empresas de Moeda Virtual*. Disponível em: https://www.dfs.ny.gov/virtual_currency_businesses [Última consulta: 23/02/2026].

UNODC. (2026). *Programa Global sobre Cibercrime (materiais de capacitação)*. Capacidades/formação em criptomoedas/darknet/provas digitais: Disponível em: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/capacitybuilding.html. Catálogo de formação 2024: https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf [Última consulta: 23/02/2026].

UNODC. (2025). *Ponto de Inflexão: Implicações Globais dos Centros de Fraude, da Banca Subterrânea e dos Mercados Online Ilegais.* Disponível em: https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html [Última consulta: 23/02/2026].

UNODC. (2024). *Relatório Anual de 2024: Secção do Crime Organizado. Gabinete das Nações Unidas contra a Droga e o Crime.* Disponível em: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Última consulta: 23/02/2026].

UNODC.1. (2024). *Redes Criminais e Estruturas Fragmentadas.* Disponível em: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Última consulta: 23/02/2026].

UNODC.2. (2024). *Casinos, Branqueamento de Capitais, Sistema Bancário Clandestino e Crime Organizado Transnacional no Leste e Sudeste Asiático: Uma Ameaça Oculta e em Aceleração.* Disponível em: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf [Última consulta: 23/02/2026].

Departamento de Justiça dos EUA. (2023). *Estados Unidos contra Binance Holdings Limited, operando sob o nome comercial Binance.com (resumo do processo).* Disponível em: https://www.justice.gov/criminal/case/united-states-v-binance-holdings-limited-dba-binancecom [Última consulta: 23/02/2026].

Departamento de Justiça dos EUA.1. (2023). *Estados Unidos contra Changpeng Zhao (resumo do processo).* Disponível em: https://www.justice.gov/criminal/case/united-states-v-changpeng-zhao [Última consulta: 23/02/2026].

14. LEGISLAÇÃO

Conselho da União Europeia. (2024) Diretiva (UE) 2024/1640 do Parlamento Europeu e do Conselho, de 31 de maio de 2024, relativa aos mecanismos que os Estados-Membros devem estabelecer para efeitos de prevenção da utilização do sistema financeiro para o branqueamento de capitais ou o financiamento do terrorismo, que altera a Diretiva (UE) 2019/1937 e altera e revoga a Diretiva (UE) 2015/849. JOUE L 2024/1640, de 19 de junho de 2024.

Organização das Nações Unidas. (2000). Nações Unidas. (2000). Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional (Resolução A/RES/55/25).

Parlamento Europeu. (2024). Sexta Diretiva contra a lavagem de capitais. Resolução legislativa do Parlamento Europeu, de 24 de abril de 2024, sobre a proposta de diretiva relativa aos mecanismos destinados a prevenir a utilização do sistema financeiro para a lavagem de capitais ou o financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849. JOUE C/2025/3790, 17 de setembro de 2025.

Parlamento Europeu e Conselho da União. (2024) Regulamento (UE) 2024/1624 do Parlamento Europeu e do Conselho, de 31 de maio de 2024, relativo à prevenção da utilização do sistema financeiro para o branqueamento de capitais ou o financiamento do terrorismo. JOUE L 2024/1624, 19 de junho de 2024.

Parlamento Europeu e Conselho da União. (2024) Regulamento (UE) n.º 2024/1620 do Parlamento Europeu e do Conselho, de 31 de maio de 2024, que cria a Autoridade de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo e altera os Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010. JOUE L 2024/1620, de 19 de junho de 2024

Parlamento Europeu e Conselho da União. (2023) Regulamento (UE) n.º 2023/1113 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo às informações que acompanham as transferências de fundos e de determinados criptoativos e que altera a Diretiva (UE) 2015/849. JOUE, L 150, 9 de junho de 2023.

Congresso dos Estados Unidos. (1977). Lei dos Poderes Económicos de Emergência Internacional, Pub. L. n.º 95-223, 91 Stat. 1625–1629 (codificada, na sua versão alterada, em 50 U.S.C. §§ 1701–1707).

Congresso dos Estados Unidos. (1970). Lei do Sigilo Bancário, Pub. L. n.º 91-508, 84 Stat. 1114

(codificada, na sua versão alterada, em 31 U.S.C. §§ 5311–5336).

15. OUTRAS FONTES NÃO CIENTÍFICAS

Binance Academy. (2024). O que é a mineração de criptomoedas ou criptomineração e como funciona? Binance. Disponível em: https://www.binance.com/es/academy/articles/what-is-crypto-mining-and-how-does-it-work [Última consulta: 23/02/2026].

Chainalysis. (2025). Tendências de 2025 em crimes relacionados com criptomoedas: volumes ilícitos apontam para um ano recorde, à medida que o crime na cadeia de

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

blocos se torna cada vez mais diversificado e profissionalizado. Disponível em: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ [Última consulta: 23/02/2026].

Equipa Editorial da Coinmetro. (2 de agosto de 2024). Crypto Mixers: Ferramentas de Privacidade e Desafios Regulatórios. *Coinmetro*. Disponível em: https://coinmetro.com/learning-lab/crypto-mixers-privacy-tools-and-regulatory-challenges [Última consulta: 23/02/2026].

Elliptic. (2024). *Prevenção do crime financeiro em criptoativos: Relatório de tipologias.* https://www.elliptic.co/hubfs/Elliptic%20Typologies%20Report%202024.pdf [Última consulta: 23/02/2026].

16. DECLARAÇÃO DE INTEGRIDADE ACADÉMICA E CIENTÍFICA

Que constitui um trabalho original, realizado por mim, sem plágio nem uso indevido de trabalhos alheios, em conformidade com as normas internacionais de integridade académica e científica.

Os dados, resultados e conclusões foram obtidos e tratados de forma honesta e rigorosa, sem invenções, falsificações nem manipulações indevidas.

A utilização de inteligência artificial ou de outras ferramentas digitais respeitou a regulamentação universitária, sem substituir a autoria intelectual nem o meu próprio julgamento académico.

Não existem conflitos de interesses que tenham influenciado o desenvolvimento ou os resultados da investigação.

Estou ciente de que o incumprimento destas declarações pode dar origem à anulação do título de doutor e às responsabilidades académicas ou legais que daí decorram.

Assumo, por minha conta, qualquer responsabilidade decorrente do incumprimento do compromisso ético aqui expresso.