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

Article de recherche

BLANCHIMENT D'ARGENT VIA LES CRYPTO-ACTIFS : EFFICACITÉ RÉGLEMENTAIRE ET FOSSÉ ENTRE TRAÇABILITÉ TECHNOLOGIQUE ET IMPUTABILITÉ JURIDIQUE DANS L'UNION EUROPÉENNE ET AUX ÉTATS-UNIS

Traduction en français à l'aide de l'IA (DeepL)

Benjamín Garcinuño Roldán
Doctorant à l'École internationale de doctorat de l'UNED (EIDUNED), membre de la Guardia Civil, avocat inscrit au Barreau de Cordoue. Titulaire d'un master en sécurité et d'une licence en droit
bgarcinun2@alumno.uned.es
https://orcid.org/0009-0005-6923-1004

Reçu le 25/02/2026
Accepté le 02/06/2026
Publié le 30/06/2026

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

Citation recommandée : Garcinuño B. (2026). Blanchiment d'argent via les crypto-actifs : efficacité réglementaire et fossé entre traçabilité technologique et imputabilité juridique dans l'Union européenne et aux États-Unis. *Revue Logos Guardia Civil*, 4(2), p. 215-252. https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

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

DÉDICACE

À Mariam, pour m’avoir fait confiance,
et pour nourrir les oiseaux qui peuplent mon esprit.
Je dois lui rappeler que le soleil continue de briller, même si elle ne le regarde pas.

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

BLANCHIMENT D'ARGENT VIA LES CRYPTO-ACTIFS : EFFICACITÉ RÉGLEMENTAIRE ET FOSSÉ ENTRE TRAÇABILITÉ TECHNOLOGIQUE ET IMPUTABILITÉ JURIDIQUE DANS L'UNION EUROPÉENNE ET AUX ÉTATS-UNIS

Résumé : Le blanchiment d'argent est un phénomène dynamique dont l'évolution est liée au contexte économique international. Les méthodes de blanchiment d'argent illicite posent de nouveaux défis réglementaires et opérationnels aux autorités et aux établissements financiers, en grande partie sous l'impulsion du développement technologique. Grâce à l'utilisation de certaines technologies récentes, elles créent un environnement de pseudonymat qui dépasse leur nature purement technique. Cette caractéristique sert d'instrument stratégique aux organisations et groupes criminels (OC) qui cherchent à sophistiquer leurs stratagèmes de blanchiment, permettant ainsi de dissimuler la traçabilité et les conséquences des préjudices sous-jacents**.** Le présent article analyse de manière critique la problématique du blanchiment de fonds illicites au moyen

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

de crypto-actifs par les OC, ainsi que les diverses stratégies employées par ces derniers pour dissimuler leur traçabilité et leur identité. Dans un premier temps, les instruments internationaux, tels que la Convention des Nations unies contre la criminalité transnationale organisée et les recommandations du Groupe d'action financière (GAFI) relatives au système de poursuite et de prévention du blanchiment de fonds illicites au moyen de crypto-actifs, sont examinés de manière systématique. Partant de ce cadre international, le présent travail s'articule autour d'une analyse comparative des cadres législatifs, sensiblement différents, relatifs au blanchiment de capitaux par le biais des crypto-actifs aux États-Unis (USA) et dans l'Union européenne (UE). La présente étude ne se limite pas à une approche descriptive du phénomène, mais souligne la nécessité de renforcer l'architecture réglementaire, en identifiant les divergences législatives significatives, les lacunes juridiques et les limites des mécanismes de surveillance.

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.

Mots-clés : crypto-actifs, blanchiment d'argent, criminalité organisée, pseudonymat numérique, réglementation financière, technologies émergentes, darknet, transparence et propriété effective.

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

ABRÉVIATIONS

AML : *Anti-Money Laundering*. En français : lutte contre le blanchiment d'argent.

AMLA : *Anti-Money Laundering Authority*. En français : Autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme.

AMLC : *Anti-Money Laundering Council*. En français : Conseil de lutte contre le blanchiment de capitaux ou d'argent.

BARIS : *Système d'interconnexion des registres de comptes bancaires*. En français : Système d'interconnexion des registres de comptes bancaires de l'Union européenne.

BC : Blanchiment d'argent.

BSA : *Bank Secrecy Act*. En français : loi sur le secret bancaire.

CDD : *Customer Due Diligence*. En français : diligence raisonnable à l'égard de la clientèle (DDC).

CEO : *Chief Executive Officer*. En français : directeur général ou président-directeur général, selon les pays.

CFT : Lutte contre le financement du terrorisme.

CFTC : *Commodity Futures Trading Commission*. En français : l'agence fédérale indépendante des États-Unis qui réglemente les marchés dérivés (contrats à terme, *swaps* et certaines options).

DAO : *Decentralized Autonomous Organization*. En français : dans le contexte de la lutte contre le blanchiment d'argent (AML/CFT), il s'agit d'une organisation native de *la blockchain* qui coordonne les décisions et gère les actifs au moyen de *contrats intelligents* et d'une gouvernance par jetons, sans direction centrale traditionnelle.

DEA : *Drug Enforcement Administration*. En français : Administration chargée de la lutte contre les stupéfiants.

États-Unis : États-Unis.

EUR : euro.

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

FBI : *Federal Bureau of Investigation*. En français : c'est l'Agence fédérale de renseignement et de sécurité intérieure des États-Unis et son principal service de police fédéral.

FinCEN : *Financial Crimes Enforcement Network*. En français, on le traduit généralement par « Réseau de lutte contre la criminalité financière ».

FT : Financement du terrorisme.

GAFI : Groupe d'action financière internationale.

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

IA : Intelligence artificielle.

IEEPA : *International Emergency Economic Powers Act*. En français : Loi sur les pouvoirs économiques d'urgence internationaux.

ICO : *Initial Coin Offering*. En français : « Offre initiale de cryptomonnaie ».

IRS : *Internal Revenue Service*. En français : Administration fiscale fédérale des États-Unis.

KYC : *Know Your Customer*. En français : « Connaissez votre client ».

MiCA : *Markets in Crypto-Assets*. En français : Règlement sur les marchés des crypto-actifs.

NCA : *National Crime Agency*. En français : Agence nationale de lutte contre la criminalité du Royaume-Uni.

NYDFS : *New York State Department of Financial Services*. En français : Département des services financiers de l'État de New York.

OC : Organisation criminelle.

PBC/FT : Prévention du blanchiment d'argent et du financement du terrorisme.

SEC : *Securities and Exchange Commission*. En français : Commission des valeurs mobilières des États-Unis.

SEPBLAC : Service exécutif de la Commission de prévention du blanchiment d'argent et des infractions monétaires.

STR : *Suspicious Transaction Report*. En français : Déclaration d'opération suspecte.

UIF : Unité de renseignement financier. Il s'agit du SEPBLAC en Espagne (Service exécutif de la Commission de prévention du blanchiment de capitaux et des infractions monétaires).

UNODC : *Office des Nations unies contre la drogue et le crime*. En espagnol : Oficina de las Naciones Unidas contra la Droga y el Delito.

UNTOC : *Convention des Nations Unies contre la criminalité transnationale organisée*. En espagnol : Convention des Nations Unies contre la criminalité transnationale organisée.

USD : *United States Dollar*, ou dollar américain.

VASP : *Virtual Asset Service Provider*. En français : prestataires de services d'actifs virtuels ou CASP dans le cadre européen.

6AMLD : Sixième directive relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

1. INTRODUCTION

Ces dernières années, les crypto-actifs ont révolutionné le monde de la finance, ouvrant la voie à l'innovation et à l'inclusion financière comme jamais auparavant. Mais ces progrès technologiques ont également donné lieu à de nouveaux défis, notamment dans le domaine de la criminalité financière. L'une des préoccupations majeures concerne l'utilisation des crypto-actifs à des fins de blanchiment de capitaux (BC) par des organisations ou des groupes criminels (OC).

Ces actifs opèrent généralement sur des réseaux décentralisés appelés « chaînes de blocs » (*blockchain*), qui garantissent des transactions transparentes et sécurisées sans recourir à un tiers centralisé tel qu'une banque (Bhutta et al., 2021). Lorsqu'une cryptomonnaie est transférée, la transaction est enregistrée sur *la blockchain*, qui fonctionne comme un registre comptable public réparti sur de nombreux ordinateurs à travers le monde (Soltani et al., 2022). Les transactions sont vérifiées par un réseau d'utilisateurs appelés « mineurs », qui sont récompensés par de nouvelles unités de crypto-actifs (Binance Academy, 2024).

Depuis des décennies, le blanchiment d'argent (BA) constitue un problème à l'échelle internationale. La dissimulation de la provenance des fonds obtenus illégalement a été l'objectif principal des organisations criminelles (OC), qui avaient pour ferme intention de leur donner une apparence légale au sein des systèmes économiques. Grâce à cette technique, les OC pouvaient investir leurs gains illégaux sans laisser de traces financières susceptibles de mener à leur découverte et à leur poursuite.

Les organisations criminelles (OC) traditionnelles sont hautement structurées, avec des hiérarchies et des rôles bien définis pour leurs membres (Enríquez Pérez, 2020) ; elles sont souvent soutenues par des responsables politiques locaux et recourent à la corruption pour éviter les démêlés avec la police (Luna Galván et al., 2021). Elles opèrent au sein de structures décentralisées qui compliquent l'identification de leurs activités (ONUDC, 2024). La structure de ces organisations criminelles est conçue pour les protéger des forces de l'ordre et réduire le risque d'infiltration ou de trahison (UNODC,1, 2024). Afin de garantir une définition commune de la criminalité organisée entre les États membres, la Convention des Nations Unies contre la criminalité transnationale organisée a été adoptée. La présente Convention définit une organisation criminelle comme un groupe structuré composé d'au moins trois personnes agissant de concert pour commettre des infractions dans le but d'en tirer un profit financier direct ou indirect (Akkoyun & Çelik, 2022).

Les organisations criminelles, qui possèdent un haut niveau de spécialisation dans l'utilisation d'outils financiers complexes, recourent de plus en plus aux monnaies virtuelles pour masquer l'origine de leurs fonds illicites (Trozze et al., 2022). Elles emploient des techniques telles que le « *layering* »[1] , les services de mixage et les transferts transfrontaliers afin de compliquer la traçabilité des fonds. (Arnone et al., 2025). L'intégration d'outils d'analyse *de la blockchain* et le renforcement des obligations KYC/PBC/FT (prévention du blanchiment de capitaux et du financement du terrorisme) permettent d'optimiser la détection et le contrôle des opérations illicites. (Rodríguez-Valencia et al., 2025).

L'article suivant aborde la problématique du blanchiment de fonds illicites par le biais des crypto-actifs par les organisations criminelles et le cadre juridique existant pour le combattre. Cette analyse inclut les recommandations du GAFI, les instruments internationaux ainsi que les réglementations des États-Unis (US) et de l'Union

[1] Le *« layering »* (ou stratification) est la deuxième phase du processus de blanchiment d'argent, dont l'objectif principal est de dissimuler l'origine illicite des fonds au moyen d'une série de transactions financières complexes, successives et souvent transfrontalières. Cette étape vise à briser la traçabilité de l'argent et à compliquer la tâche des autorités chargées de reconstituer le parcours initial des fonds.

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

européenne (UE) visant à prévenir le blanchiment via les crypto-actifs par les organisations criminelles. Le présent travail examine les traités internationaux et les lois nationales des États-Unis et de l'Europe qui visent à prévenir le blanchiment par les organisations criminelles.

Partant de ce constat, nous développons dans le présent article une analyse comparative des modèles réglementaires des États-Unis et de l'UE, dans le but d'identifier leurs forces et leurs faiblesses et de formuler des critères juridiques d'évaluation. De même, le présent travail soutient l'efficacité de l'effort institutionnel visant à lutter contre le blanchiment d'argent via les crypto-actifs, dans la mesure où celui-ci ne repose pas uniquement sur l'élaboration formelle des cadres réglementaires. Par ailleurs, son degré d'efficacité dépend de la capacité réelle à prévenir, détecter, attribuer et sanctionner les comportements illicites dans un environnement caractérisé par le pseudonymat, la décentralisation technologique et la dimension transnationale du phénomène.

La principale contribution de cette étude réside dans l'identification de l'existence d'un fossé structurel entre la traçabilité technique des transactions sur *la blockchain* et leur attribution juridique effective. Par conséquent, les modèles conventionnels de prévention, de détection et de sanction, intégrant des capacités technologiques dans les systèmes réglementaires, doivent être repensés.

2. MÉTHODOLOGIE DE RECHERCHE

Le présent document adopte une approche analytique descriptive. L'analyse sera multidimensionnelle et portera sur la réglementation, la littérature et les informations disponibles afin d'évaluer les mesures de prévention du blanchiment de crypto-actifs mises en œuvre par les organisations criminelles. L'examen exploratoire de la littérature existante (livres, revues, articles, etc.) permettra de mieux comprendre le concept, la nature et les meilleures façons de résoudre ce problème.

Cette approche constitue la méthodologie la plus appropriée pour mener cette recherche en raison du manque d'informations et de l'absence d'articles traitant de manière approfondie des recommandations du GAFI, des conventions internationales et des législations nationales des États-Unis et de l'Europe concernant la problématique du blanchiment de crypto-actifs par les organisations criminelles.

De même, ce travail intègre une dimension analytique à caractère constructif, visant à identifier les limites structurelles du cadre juridique actuel dans les environnements numériques décentralisés.

3. ANALYSE DE L'UTILISATION (ABUSIVE) DES CRYPTO-ACTIFS PAR LES ORGANISATIONS CRIMINELLES

La prolifération des services bancaires clandestins et d'autres réseaux de blanchiment en ligne a donné naissance à des canaux de transfert financier plus anonymes (Europol, 2022). Les crypto-actifs présentent un risque d'utilisation abusive par des criminels ; en conséquence , le secteur développe de nouvelles formes complexes et des services de mixage entre pairs. Cela crée les conditions propices à la dissimulation des transactions, à l'analyse décentralisée régulière de *la blockchain* et à l'émergence récente de nouveaux réseaux peer-to-peer susceptibles d'être utilisés dans le cadre d'activités illégales (Hinojal, 2023). Ces évolutions rendront nettement plus difficile l'identification des activités des organisations criminelles qui utilisent les cryptomonnaies conventionnelles pour dissimuler des profits illicites (Fu et al., 2025).

Le trafic de drogue, d'armes et d'autres marchandises illégales est une activité lucrative, dans la mesure où ces fonds illicites peuvent être facilement transférés vers et depuis des organisations criminelles partout dans le monde (Sudan et al., 2023). En effet, au-delà des escroqueries, les crypto-actifs ont été associés à presque tous les types de cybercriminalité, depuis les services sur le *deep web*[2] ou *le darknet*[3] jusqu'au vol et à la fraude sous leurs multiples formes.

Les crypto-actifs ont été utilisés dans diverses activités des organisations criminelles, notamment le blanchiment d'argent, les attaques *par ransomware*[4] et la fraude en ligne. Afin de lutter contre ces pratiques illicites, les forces de l'ordre ont bénéficié d'une vue d'ensemble de la littérature existante sur le sujet (Trozze et al., 2022). La recherche sur l'utilisation abusive par les organisations criminelles reste encore limitée par rapport à d'autres thèmes de recherche sur les crypto-actifs et *la blockchain*. Parmi les activités illégales menées par les organisations criminelles à l'aide de monnaies numériques figurent le blanchiment (produit du crime), les *ransomwares* et les marchés noirs (Alessi Longa, 2025).

Sept catégories ont été identifiées, chacune résumant un modèle spécifique de comportement criminel dans l'utilisation des crypto-actifs et ses implications pour les mécanismes de prévention, de détection et d'intervention :

(1) le financement du terrorisme, (2) sur le dark *web*, (3) sur les marchés du *deep web* ou *du darknet*, (4) dans la cybercriminalité, (5) dans le trafic de drogue, (6) dans la traite des êtres humains, (7) et dans la corruption.

Nous concentrerons notre recherche sur l'option 2 :

4. CRYPTO-ACTIFS ET BLANCHIMENT D'ARGENT PAR LES ORGANISATIONS CRIMINELLES

Les crypto-actifs reçus par des adresses illicites en 2023 se sont élevés à 46 100 millions de dollars américains (Chainalysis, 2025). En 2024, la valeur des fonds reçus par des adresses illicites a chuté à 40,9 milliards de dollars. Mais les chiffres de 2024 sont provisoires et pourraient facilement dépasser les 51 milliards de dollars (Atlam et al., 2024).

Si certains affirment que les crypto-actifs entraînent des coûts élevés en matière d'information et de contrôle, les transactions sont généralement moins chères et plus rapides que celles effectuées en monnaies fiduciaires, puisqu'il n'y a pas d'intermédiaires entre acheteurs et vendeurs (Medranda Morales & Arcos Argudo, 2023). Mais ces mêmes caractéristiques ont été exploitées par les organisations criminelles à des fins de blanchiment. En particulier, trois caractéristiques des crypto-actifs réduisent considérablement les coûts de transaction liés à ces activités illégales.

Tout d'abord, la nature décentralisée des crypto-actifs permet aux utilisateurs d'échanger de la valeur directement entre eux sans avoir recours à des intermédiaires.

---

[2] Le deep web (ou web profond) est la partie d'Internet qui n'est pas indexée par les moteurs de recherche classiques, tels que Google, Bing ou Yahoo. Cela signifie que son contenu ne peut être trouvé par le biais de recherches normales et n'est accessible que si l'on connaît directement l'adresse, si l'on dispose d'une autorisation ou si l'on utilise des identifiants spécifiques.

[3] Le darknet est une partie spécifique et délibérément cachée d'Internet à laquelle on ne peut accéder qu'à l'aide de logiciels, de configurations ou de protocoles spéciaux garantissant l'anonymat, tels que Tor, I2P ou Freenet. Il n'est pas indexé par les moteurs de recherche classiques et est conçu pour protéger l'identité et la localisation des utilisateurs et des serveurs.

[4] Un *ransomware* est un type de logiciel malveillant (*malware*) conçu pour bloquer, chiffrer ou rendre inutilisables les systèmes informatiques d'une victime, dans le but d'exiger une rançon financière — généralement en cryptomonnaies — en échange du rétablissement de l'accès aux données ou aux systèmes.

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

Comme indiqué précédemment, les réglementations traditionnelles visant à lutter contre le blanchiment d'argent visent à encadrer les intermédiaires qui effectuent des opérations afin de prévenir les transferts illégaux (Longa, 2025) ; or, l'absence d'interactions en face à face dans les transactions de crypto-actifs rend plus difficile l'identification des parties concernées (Montoya Arrubla, 2025). Deuxièmement, bien que toutes les transactions soient enregistrées et traçables sur la *blockchain*, il n'existe aucun lien explicite avec les personnes physiques ou morales réelles qui se cachent derrière elles. Les crypto-actifs fonctionnent selon un système pseudonyme dans lequel seule la clé publique (une chaîne aléatoire de chiffres) est connue, tandis que la clé privée reste secrète.

Cela rend considérablement plus difficile l'association d'une identité réelle à une adresse de cryptomonnaie (Béres et al., 2021). Cependant, les utilisateurs peuvent créer plusieurs portefeuilles de cryptoactifs électroniques avec des adresses publiques différentes, ce qui complique la traçabilité en cas de soupçon de blanchiment (Atlam et al., 2024).

Enfin, la rapidité des transactions en crypto-actifs et leur facilité d'utilisation constituent un avantage par rapport aux méthodes traditionnelles de blanchiment, telles que les espèces. Contrairement à la monnaie fiduciaire, qui est limitée par son poids et sa taille, les crypto-actifs peuvent être stockés en quantités illimitées sur une clé USB et envoyés à n'importe qui dans le monde en quelques minutes. La malléabilité des transactions facilite le contournement des mesures réglementaires, puisqu'il est possible de fractionner une transaction importante en plusieurs transactions plus modestes (Koelbing et al., 2024). Cette flexibilité opérationnelle est essentielle et renforce le BC pour les OC opérant sur les marchés des crypto-actifs. Ces organisations génèrent un volume important de crypto-actifs, qu'elles doivent transformer en fonds d'apparence légale.

Ce processus implique généralement une série de transactions financières complexes qui font transiter les fonds par de multiples comptes et juridictions, rendant difficile la traçabilité de leur origine. Cela permet aux organisations criminelles de continuer à opérer dans l'illégalité et de dissimuler les profits issus du trafic de drogue (GAFI, 2022). Les organisations criminelles qui utilisent le *deep web* sont passées maîtres dans le blanchiment des crypto-actifs, lesquels peuvent être transférés instantanément d'un compte à l'autre et sont difficiles à tracer (Holt et al., 2023). Ces organisations criminelles font souvent appel à des facilitateurs professionnels (avocats, comptables, banquiers, etc.) pour compliquer la traçabilité de leurs fonds illicites.

Les organisations criminelles peuvent conserver à titre d'investissement les crypto-actifs qu'elles reçoivent lors d'opérations sur le marché des cryptomonnaies. Ceux-ci sont utilisés pour blanchir d'autres devises illicites, tant en ligne que dans le monde réel (Arnone et al., 2025). Ceux qui ne sont pas conservés à titre d'investissement sont blanchis et injectés dans l'économie légale. Par exemple, la police néerlandaise a découvert qu'un modérateur d'une place de marché cryptographique exploitait ses contacts pour échanger des bitcoins contre des espèces (Ministère de l'Intérieur, 2024).

En Asie de l'Est et du Sud-Est, les organisations dites « *point* runners » ou « *moving* ants » sont utilisées pour blanchir des fonds illicites, en recrutant de nombreuses personnes (souvent des jeunes sans emploi) qui prêtent leurs comptes bancaires et créent des sociétés fictives afin de dissimuler la source et la destination des fonds illicites (ONUDC, 2025). Ces réseaux font transiter les fonds par de multiples comptes bancaires ou de crypto-actifs et par des casinos en ligne, où ils sont déguisés en gains légitimes de casino (Langdale, 2024).

Maintenant que les autorités ont une meilleure connaissance des paiements par des tiers (à la suite de *l'« Opération Chain* Break » et d'autres opérations similaires menées en Chine) (FinCEN, 2025), les organisations criminelles ont de plus en plus recours aux

crypto-actifs pour leurs opérations de jeux d'argent illégaux, ce qui pose de sérieux défis aux enquêteurs (Europol, 2024). Par exemple, des casinos et des opérateurs de *junkets*[5] titulaires d'une licence aux Philippines ont été impliqués dans le blanchiment d'environ 81 millions de dollars dérobés lors d'une cyberattaque de 2016 attribuée au groupe Lazarus contre la Banque centrale du Bangladesh (Langdale, 2024). Bien que ces fonds soient passés par des banques et des sociétés de transfert de fonds, il s'est avéré extrêmement complexe de les retracer une fois qu'ils sont parvenus entre les mains des opérateurs de voyages organisés vers les casinos (AMLC, 2023).

Les cartels mondiaux de la drogue ont été accusés par la DEA d'utiliser *Binance*,[6] , la plus grande plateforme d'échange de cryptomonnaies, pour blanchir entre 15 et 40 millions de dollars au cours de diverses transactions (DEA, 2025). Selon les rapports de la DEA, *Binance* collabore avec les enquêteurs alors que la plateforme fait l'objet d'un examen minutieux suite à diverses plaintes.

Ces mécanismes sophistiqués posent de nouveaux défis en matière de détection et d'enquête en raison du nombre de transactions et de leur nature transfrontalière, ce qui exige une plus grande transparence financière, une coopération internationale et des cadres réglementaires plus solides pour lutter contre ces délits (Legrand & Leuprecht, 2021).

5. MÉTHODES LES PLUS COURANTES DE BLANCHIMENT DE CRYPTO-ACTIFS UTILISÉES PAR LES ORGANISATIONS CRIMINELLES

5.1. CONSIDÉRATIONS GÉNÉRALES DU POINT DE VUE DE LA DOGMATIQUE DU BLANCHIMENT DE CAPITAUX

Le phénomène ainsi conceptualisé met en évidence que les différentes techniques employées par les organisations criminelles s'inscrivent dans les phases classiques du blanchiment de capitaux, en particulier le placement, la stratification et l'intégration.

Ces pratiques décrites dans la section précédente sont celles qui soulèvent des problématiques liées à la qualification pénale, à l'attribution de la responsabilité et à la reconstitution du parcours financier des fonds illicites. Cela est particulièrement vrai dans un environnement caractérisé par la pseudonymité et la décentralisation technologique, comme c'est le cas des crypto-actifs.

5.2. TECHNIQUES LIÉES À LA PHASE D'INTÉGRATION : LE « *SMURFING* »

La pratique connue sous le nom de « *smurfing* », « pitufeo » ou « menudeo » consiste à intégrer dans le système financier, de manière variée et par petits montants, des fonds provenant d'activités illicites, de l'argent issu du trafic de drogue, de paiements frauduleux, de la corruption ou de profits provenant de l'exploitation sexuelle (Isolauri & Ameer, 2023). Cette technique, utilisée dans la finance traditionnelle, semble s'être étendue au monde des crypto-actifs (Koelbing et al., 2024).

D'un point de vue pénal, ce type de pratiques peut s'inscrire dans la phase d'intégration du blanchiment de capitaux. Il s'agit clairement de l'intention d'introduire

[5] Les opérateurs de « junkets » sont des intermédiaires spécialisés qui agissent entre les casinos et les joueurs VIP ou « high-rollers », notamment sur des marchés tels que Macao, Las Vegas, Singapour et d'autres centres internationaux de jeux. Leur rôle principal consiste à recruter, transporter, financer et gérer des clients à forte valeur ajoutée afin qu'ils jouent dans certains casinos.

[6] Binance est la plus grande plateforme d'échange de cryptomonnaies au monde en termes de volume de transactions et de nombre d'utilisateurs ; elle a été fondée en 2017 par Changpeng Zhao (CZ) et Yi He. Il s'agit d'une plateforme centralisée (CEX) qui permet d'acheter, de vendre, d'échanger et de conserver des actifs numériques.

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

des fonds illicites dans le système financier officiel, par le biais de leur fractionnement, afin de contourner les mécanismes de contrôle. D'un point de vue juridique, cela soulève des questions importantes concernant l'application des seuils réglementaires et l'efficacité des systèmes de détection automatisés.

5.3. TECHNIQUES LIÉES À LA PHASE DE STRATIFICATION : DISSIMULATION ET DISSOCIATION DE L'ORIGINE ILLÉGALE

5.3.1. Portefeuille de crypto-actifs (portefeuilles de taille moyenne) (medium wallets ou mid-size wallets)

Une méthode courante de blanchiment d'argent (BC) impliquant des crypto-actifs consiste à utiliser des portefeuilles intermédiaires. Cette technique de stratification vise à dissimuler le lien entre les fonds illicites et leur entrée ultérieure dans le système financier légal (Elliptic, 2024). Par conséquent, les portefeuilles intermédiaires sont utilisés par les criminels sur les *plateformes d'échange*, qu'elles soient soumises ou non à l'obligation de KYC.

D'un point de vue théorique, les comptes intermédiaires et leur utilisation sont directement liés à la phase de stratification du blanchiment d'argent, car ils visent à entraver la traçabilité des fonds illicites. Ces comportements posent des défis majeurs en matière d'attribution objective et d'identification du bénéficiaire effectif, en particulier lorsqu'il n'y a pas de points de contact avec des intermédiaires tenus de procéder à l'identification.

5.3.2. Portefeuilles de crypto-actifs de consolidation

Les portefeuilles de consolidation, qui regroupent et combinent des fonds provenant de diverses sources, constituent une autre tendance à prendre en compte. Ce modèle de consolidation peut révéler des tentatives visant à dissimuler l'origine illicite des fonds avant de les transférer vers des bourses ou d'autres lieux de retrait d'espèces (Chiang, 2024).

D'un point de vue juridique, ces structures pourraient être considérées comme des instruments conçus pour renforcer la dissimulation de l'origine illicite des fonds. Cette circonstance a une incidence directe sur la configuration type du délit de blanchiment d'argent dans sa modalité de dissimulation ou de couverture.

5.3.3. Services de mixage, cryptomonnaies axées sur la confidentialité et ponts

L'objectif du mélange et du brassage est de disséminer d'importantes quantités de cryptomonnaies en les répartissant dans de multiples directions (Gorjón, 2023). Les « mélangeurs » sont des particuliers ou des entreprises qui répartissent les fonds entre les participants et les mélangent à des revenus licites afin de masquer la traçabilité et l'identification des propriétaires (Coinmetro Editorial Team, 2024).

Les problèmes spécifiques liés à la qualification pénale lors de la phase de dissimulation des cryptomonnaies, soulevés par le recours à des services de mélange, sont précisément conçus pour entraver la traçabilité des fonds. Par conséquent, cette problématique remet en question la portée des obligations de diligence raisonnable des prestataires de services d'actifs virtuels (VASP) ou CASP dans le cadre européen. Cette situation est prévue à l'article 13 de la directive (UE) 2015/849, en particulier lorsque ces prestataires opèrent dans des juridictions où la surveillance est limitée, voire inexistante.

Les cryptomonnaies axées sur la confidentialité exacerbent les difficultés liées à l'attribution des transactions, en renforçant le pseudonymat au niveau de l'identité. Cela

engendre une limitation opérationnelle essentielle en matière de preuve dans le cadre des procédures pénales, notamment en ce qui concerne le lien entre des adresses et des personnes physiques ou morales spécifiques. Les cryptomonnaies axées sur la confidentialité sont devenues populaires auprès de ceux qui souhaitent passer inaperçus (Cremers et al., 2024).

Le transfert d'actifs entre différentes *blockchains* est une technique connue sous le nom de « ponts cryptographiques », méthode ou outil de plus en plus populaire pour le BC.

D'un point de vue juridique, l'utilisation de ponts entre *blockchains* accentue la dimension transnationale du BC, en soulevant des problèmes de compétence juridictionnelle et de coopération internationale, ainsi qu'une contrainte opérationnelle supplémentaire dans la reconstitution du parcours financier des fonds.

5.4. ESPACES CRIMINOGÈNES ET FACILITATEURS : LES MARCHÉS DU *DARKNET*

Les marchés du *darknet* sont des sites en ligne cachés auxquels on accède via des logiciels spécifiques (tels que Tor) et où les paiements s'effectuent en crypto-actifs anonymes. Ces marchés facilitent le commerce de biens et de services illégaux et offrent aux blanchisseurs un moyen de convertir des fonds illicites en crypto-actifs et vice versa (Jordá et al., 2024). Il est extrêmement difficile de déterminer avec précision le montant des fonds illicites blanchis à l'aide de cet actif virtuel (Alessi Longa, 2025).

Sur le darknet, *Silk Road* était la place de marché la plus populaire fonctionnant sur le réseau *Tor*, car elle permettait des transactions anonymes en crypto-actifs. Bien qu'il ait tenté de préserver son pseudonymat, son fondateur, Ulbricht, a été arrêté par le FBI en 2013 et finalement condamné pour plusieurs chefs d'accusation.

Compte tenu de l'ampleur des opérations de blanchiment, il convient d'examiner le cadre juridique existant afin de lutter contre le blanchiment de crypto-actifs par les organisations criminelles. Ces environnements accentuent les difficultés structurelles rencontrées par les autorités pour intervenir et posent des défis réglementaires et opérationnels tant au niveau de l'obtention de preuves numériques que de l'identification des acteurs impliqués, ce qui a une incidence directe sur l'efficacité des poursuites pénales menées par les autorités chargées de la lutte contre le blanchiment d'argent. Cette affaire a mis en évidence les défis liés à la réglementation et à la surveillance du *deep web* (Hemdani, 2025).

5.5. CONSIDÉRATION DOGMATIQUE FINALE

Toutes ces techniques mettent en évidence les limites du droit pénal conventionnel à s'adapter à des structures technologiques décentralisées. Cela soulève des questions quant à la délimitation des infractions pénales et à l'efficacité des réponses normatives dans un environnement numérique en constante évolution.

6. CADRES JURIDIQUES DE LUTTE CONTRE LE BLANCHIMENT DE CRYPTO-ACTIFS PAR LES ORGANISMES DE CRÉDIT

Les cadres juridiques relatifs aux crypto-actifs sont très fragmentés à l'échelle mondiale, certains pays les interdisant totalement tandis que d'autres les adoptent sans réserve. Des efforts ont été déployés dans le cadre de la Convention des Nations unies contre la criminalité transnationale organisée (UNTOC) pour lutter contre la criminalité transnationale organisée.

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

6.1. CONVENTION DES NATIONS UNIES CONTRE LA CRIMINALITÉ ORGANISÉE TRANSNATIONALE

La Convention de l'UNTOC de 2000 est le principal instrument juridique international permettant de relever les défis posés par la criminalité organisée transnationale. Elle offre un ensemble d'outils permettant aux États d'élaborer des politiques et des cadres juridiques visant à prévenir et à combattre les différentes formes de criminalité organisée, telles que le blanchiment d'argent lié aux crypto-actifs (Kabra & Gori, 2025). Cette convention revêt une importance particulière dans la mesure où ces actifs virtuels jouent un rôle de plus en plus important dans l'univers financier des organisations criminelles. L'UNTOC peut soutenir la répression et la prévention du blanchiment de crypto-actifs grâce à l'élaboration de cadres juridiques plus solides, à la coopération internationale et à l'application de normes communes pour lutter contre les transactions illégales portant sur ces actifs virtuels (Wang & Hsieh, 2023).

Ses articles 1, 13, 16 et 18 régissent la coopération transfrontalière en matière d'entraide judiciaire, d'extradition et d'échange d'informations. Étant donné que les transactions portant sur des crypto-actifs peuvent impliquer plusieurs juridictions, l'accent mis par la Convention des Nations unies contre la criminalité transnationale organisée (UNTOC) sur la coopération internationale est essentiel pour identifier et traduire en justice les organisations criminelles qui abusent de ces actifs virtuels. Par exemple, l'Agence nationale contre la criminalité (NCA) du Royaume-Uni a démantelé un vaste réseau de criminalité organisée lié aux cryptomonnaies, d'une valeur de plusieurs milliards de dollars, baptisé « Opération Déstabiliser » (Anggriawan & Susila, 2024).

Ce réseau s'adressait à un large éventail d'organisations criminelles, allant de riches Russes et de personnalités influentes à l'échelle mondiale à des cybercriminels et des trafiquants de drogue. La NCA a identifié deux organisateurs du crime russophones, « Smart » et « TGR », comme étant les commanditaires. À ce jour, son enquête a conduit à 84 arrestations et à la saisie de plus de 20 millions d'euros en espèces et en crypto-actifs (UNODC2, 2024). Cette opération couronnée de succès a été rendue possible grâce à la collaboration des signataires de la convention, parmi lesquels figurent l' , la Police métropolitaine du Royaume-Uni, la *Direction centrale de la police judiciaire* française, le Bureau du contrôle des avoirs étrangers du Trésor américain, l'Agence antidrogue et le FBI (FATF et al., 2025).

L'article 34 de la Convention des Nations unies contre la criminalité transnationale organisée (UNTOC) encourage les États à adopter des mesures législatives compatibles pour prévenir le blanchiment d'argent, ce qui est essentiel pour faire face aux risques croissants de criminalité financière liés aux crypto-actifs. Par exemple, le GAFI exige des mesures de « KYC » (connaissance du client) et de diligence raisonnable à l'égard de la clientèle pour identifier et signaler les transactions suspectes portant sur des crypto-actifs, lesquelles doivent être mises en œuvre dans tous les pays, indépendamment de leurs législations locales. (GAFI, 2024).

La Convention des Nations unies contre la criminalité transnationale organisée (UNTOC) soutient l'élaboration de normes internationales, en aidant les pays à développer des capacités optimisées en matière de cybersécurité et d'enquête afin de détecter les infractions liées aux crypto-actifs. ONUDC (2026). Par exemple, les canaux d'échange d'informations de l'UNTOC aident les services répressifs de l'UE, tels qu'Europol, à tracer les transactions illégales portant sur ces actifs virtuels. Cela peut impliquer, à cet égard, Eurojust, l'agence de l'UE chargée de la coopération judiciaire, afin de garantir des poursuites transfrontalières efficaces.

Dans ce contexte, l'UNTOC propose une approche internationale visant à lutter contre le blanchiment des crypto-actifs, en favorisant la coopération internationale,

l'harmonisation juridique et le renforcement des capacités en matière d'application de la réglementation.

6.2. RECOMMANDATIONS DU GROUPE D'ACTION FINANCIÈRE INTERNATIONALE

Le GAFI a établi un ensemble complet de normes visant à atténuer et à lutter contre le blanchiment de capitaux et le financement du terrorisme (BC/FT), qui couvre les actifs virtuels et les prestataires de services d'actifs virtuels (VASP). D'un point de vue juridique, le GAFI définit les « actifs virtuels » et les « prestataires de services d'actifs virtuels » afin de garantir une application cohérente et uniforme de ses normes. Les actifs virtuels sont une représentation numérique de valeur qui peut être négociée ou transférée par voie numérique et qui peut être utilisée pour effectuer des paiements ou des investissements (GAFI, 2023).

Les VASP désignent toute personne physique ou morale non couverte par ailleurs par les Recommandations et qui, à titre professionnel, exerce une ou plusieurs des activités suivantes : l'échange entre des actifs virtuels et des monnaies fiduciaires ; entre une ou plusieurs formes d'autres actifs virtuels ; le transfert d'actifs virtuels ; la conservation et/ou la gestion d'actifs virtuels ou d'instruments permettant de réguler les actifs virtuels ; et la participation et la fourniture de services financiers liés à l'offre et/ou à la vente d'un actif virtuel par un émetteur (GAFI, 2021).

D'un point de vue juridique, la Recommandation n° 15 traite spécifiquement des actifs virtuels, en stipulant que les pays doivent identifier et atténuer les risques de blanchiment de capitaux et de financement du terrorisme liés aux actifs virtuels et aux prestataires de services d'actifs virtuels (VASP). Le GAFI exige la mise en œuvre de mesures de vigilance à l'égard de la clientèle (CDD), la tenue de registres, la déclaration des opérations suspectes (STR), des contrôles internes et des programmes de conformité, ainsi que des sanctions (FATF.1, 2023). De même, la recommandation n° 16 impose aux VASP de collecter, conserver et transmettre les informations relatives au donneur d'ordre et au bénéficiaire lors des transferts d'actifs virtuels dépassant un certain seuil (1 000 USD/EUR). Cette règle est parfois appelée « règle du voyage ».[7]

Cette règle vise à prévenir l'utilisation des actifs virtuels à des fins illégales et à garantir la transparence des transactions, dans la mesure où elle impose aux VASP de partager ces informations avec d'autres entités assujetties. La règle du voyage pour les actifs virtuels a été une priorité pour le GAFI, qui continue de faire pression sur les pays pour qu'ils la mettent en œuvre et la fassent respecter (Mollaahmetoğlu & Baykut, 2021).

Le GAFI met régulièrement à jour ses recommandations sur les actifs virtuels afin de s'adapter à l'évolution des risques et aux innovations technologiques dans le domaine des actifs virtuels. Les pays devraient intégrer ces règles dans leurs lois et réglementations nationales. Le GAFI continue de surveiller la mise en œuvre de ces normes à l'échelle mondiale et exhorte les juridictions à donner la priorité à leur mise en œuvre effective (Teng et al., 2026).

[7] La règle de voyage est une obligation établie par le Groupe d'action financière internationale (GAFI/FATF) qui exige des établissements financiers et des prestataires de services d'actifs virtuels (VASP) qu'ils transmettent des informations sur l'initiateur et le bénéficiaire lors de tout transfert de fonds ou de crypto-actifs. Son objectif est de garantir la traçabilité et de permettre aux autorités d'identifier les parties impliquées dans des transactions susceptibles d'être liées au blanchiment d'argent, au financement du terrorisme ou à d'autres infractions graves.

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

7. MODÈLES RÉGLEMENTAIRES TRANSATLANTIQUES EN MATIÈRE DE BLANCHIMENT D'ARGENT AVEC DES CRYPTO-ACTIFS : ÉVALUATION COMPARATIVE ÉTATS-UNIS – UE

7.1. ÉTATS-UNIS

Aux États-Unis, il n'existe pas de cadre réglementaire unifié pour les crypto-actifs ; en revanche, plusieurs agences fédérales et étatiques supervisent ces actifs virtuels. La *Securities and Exchange Commission* (SEC), ou Commission américaine des opérations boursières, réglemente les valeurs mobilières et a considéré de nombreux crypto-actifs et offres initiales de pièces (ICO) comme des valeurs mobilières. Dans l'affaire SEC c. *Decentralized Autonomous Organization* (DAO), elle a estimé que les crypto-actifs constituaient des valeurs mobilières et qu'ils étaient donc soumis à la réglementation de la SEC (Lom & Hashmall, 2021). La *Commodity Futures Trading Commission* (CFTC), l'agence fédérale indépendante américaine chargée de réglementer les marchés dérivés, considère le bitcoin et d'autres actifs virtuels comme des matières premières et réglemente les marchés dérivés et à terme sur les crypto-actifs (Hinojal, 2023).

Le *Financial Crimes Enforcement Network* (FinCEN), ou Réseau de lutte contre la criminalité financière, contrôle les plateformes d'échange de cryptomonnaies et les fournisseurs de portefeuilles électroniques en tant qu'opérateurs de transfert de fonds ; ceux-ci doivent se conformer aux réglementations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (PBC/FT) ainsi qu'aux obligations de connaissance du client (KYC). *L'Internal Revenue* Service (IRS), ou Agence fédérale américaine des impôts, traite les crypto-actifs comme des biens à des fins fiscales, et les gains et pertes sont soumis à l'impôt sur les plus-values (Baer et al., 2023). La réglementation tend à être décentralisée ; des États comme New York ont leurs propres lois (*BitLicense*),[8] tandis que d'autres ont des politiques plus souples ou imprécises.

La *BitLicense* est une licence d'exploitation qui impose aux opérateurs des règles plus strictes en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (PBC/FT). En Californie, la loi exige que les opérateurs de bitcoins disposent de réserves équivalentes à celles des banques pour couvrir les pertes, mais la Caroline du Nord travaille encore sur des projets de loi visant à réglementer les bitcoins et ne dispose d'aucune directive en vigueur (NYDFS, 2024–2026).

Le ministère public des États-Unis a ouvert une procédure pénale contre *Rule et Nysewander*[9] pour avoir conspiré avec d'autres personnes afin de blanchir les gains illicites issus d'escroqueries sentimentales en ligne, d'escroqueries par e-mail ciblant les entreprises, d'escroqueries immobilières et d'autres fraudes via des crypto-actifs (Lim & Choi, 2025).

Selon l'acte d'accusation du ministère public des États-Unis, ils avaient procédé à la conversion des fonds illicites en crypto-actifs et les avaient transférés vers des comptes contrôlés par leurs complices aux États-Unis et à l'étranger. Cela témoigne d'une stratégie visant à dissimuler l'origine illicite des fonds et à entraver leur traçabilité. De même, lors de l'ouverture de comptes et de leurs opérations auprès de banques et de plateformes *d'échange* de cryptomonnaies, *Rule et Nysewander* auraient fait de fausses déclarations

[8] La *BitLicense* est une licence réglementaire obligatoire délivrée par le Département des services financiers de l'État de New York (NYDFS) aux entreprises exerçant des activités liées aux cryptomonnaies ou aux actifs virtuels dans l'État de New York ou avec des résidents de New York. Elle a été introduite en 2015 par le règlement 23 NYCRR Part 200.

[9] Il s'agit de deux hommes (originaires du Nevada et de Caroline du Sud) qui ont été inculpés puis condamnés pour avoir participé à un complot de blanchiment d'argent via des cryptomonnaies, selon le ministère américain de la Justice.

et omis des informations pertinentes afin de contourner les contrôles et les mesures de sécurité propres à ces institutions.

À la suite de ces agissements, dans le cadre de ce complot présumé, eux-mêmes et leurs complices ont blanchi plus de 2,4 millions de dollars américains. Finalement, tous deux ont été reconnus coupables et pourraient encourir jusqu'à 20 ans de prison fédérale pour chaque chef d'accusation de blanchiment d'argent (Farrukh et al., 2025).

De même, en août 2024, Lam et Serrano ont été inculpés pour le vol de crypto-actifs d'une valeur de 230 millions de dollars américains (Trozze et al., 2022).

Les procureurs américains se sont également intéressés à *Binance*, la société qui exploite la plus grande plateforme mondiale d'échange de crypto-actifs, *Binance.com*. L'entreprise a plaidé coupable et versera plus de 4 milliards de dollars pour mettre fin à l'enquête du ministère de la Justice concernant des violations de la loi sur le secret bancaire (BSA), pour ne pas s'être enregistrée en tant que transmetteur de fonds, et de la loi sur les pouvoirs économiques d'urgence internationaux (IEEPA) (ministère américain de la Justice, 2023).

Le Canadien Changpeng Zhao, fondateur et ancien PDG de *Binance*, a également plaidé coupable de ne pas avoir mis en place un programme efficace de lutte contre le blanchiment d'argent (PBC/FT ou AML), en violation de la loi BSA. Dans le cadre de l'accord de plaidoyer, M. Zhao a démissionné de son poste de PDG de Binance (Ministère américain de la Justice.1, 2023).

Bien que les procureurs américains aient réussi à poursuivre en justice les blanchisseurs d'argent et les plateformes *d'échange* de cryptomonnaies, le marché des crypto-actifs nécessite encore davantage de transparence afin de protéger les investisseurs potentiels (Anguren et al., 2023). Il y a quelques décennies, l'essor du commerce électronique a donné lieu à des cadres juridiques novateurs ; aujourd'hui, ces actifs virtuels et leurs multiples formes méritent un accompagnement similaire. L'élaboration de règles claires régissant la vente de certaines cryptomonnaies et de certains fonds cryptos pourrait apporter la clarté dont on a tant besoin (Blanco Barón, 2025).

En l'absence d'un cadre réglementaire plus abouti, se fier uniquement aux mesures coercitives d'organismes tels que la SEC ne suffit pas pour atteindre ses objectifs réglementaires. En fin de compte, ces mesures punitives peuvent nuire aux investisseurs mêmes que la SEC cherche à protéger et freiner l'investissement dans des entreprises prometteuses. Parmi les réglementations proposées pour les crypto-actifs figure le projet de loi contre le blanchiment d'actifs numériques, qui vise à prévenir d'autres délits liés aux actifs virtuels, tout en mettant l'accent sur les acteurs qui effectuent les transactions (mineurs, validateurs, etc.) (Warren & Marshall, 2022).

D'un point de vue juridique, le système américain se caractérise par sa nature segmentée et réactive, car il implique de multiples agences aux compétences interdépendantes. La flexibilité réglementaire qu'offre cette structure peut entraîner des problèmes de cohérence normative et d'éventuels chevauchements de compétences.

Cette approche présente des limites en matière de prévention *ex ante* en ce qui concerne les cryptomonnaies, dans la mesure où son action se concentre essentiellement sur des mécanismes de *contrôle* a posteriori, une fois l'infraction commise. L'absence d'un cadre réglementaire unifié empêche également l'application uniforme des obligations de conformité par les prestataires de services d'actifs virtuels (VASP), ce qui, dans ce contexte, pourrait créer des risques réglementaires.

7.2. UNION EUROPÉENNE

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

À l'heure actuelle, l'UE ne dispose pas d'un cadre juridique harmonisé pour les crypto-actifs dans tous les États membres. Cependant, la Commission européenne a proposé certaines mesures, telles que la sixième directive anti-blanchiment (6AMLD), qui obligerait les entreprises travaillant avec des crypto-actifs à s'enregistrer auprès des autorités nationales.

Elles devraient également respecter les règles de lutte contre le blanchiment de capitaux et signaler toute transaction suspecte. L'objectif de la 6AMLD est de combler les lacunes juridiques des législations nationales des pays de l'UE en établissant des définitions cohérentes pour le blanchiment de capitaux et les actifs virtuels dans toute l'UE (Parlement européen, 2024).

Afin d'établir une approche uniforme de la réglementation des transactions sur les crypto-actifs dans toute l'UE, la Commission européenne a proposé le règlement du Parlement européen et du Conseil sur les marchés des crypto-actifs ainsi que la directive modificative. Cet ensemble de règles, appelé MiCA ([10]), vise à mettre en place un cadre de surveillance comprenant des règles applicables aux émetteurs, aux prestataires de services et aux acteurs du marché secondaire.

S'appuyant sur ces réglementations MiCA et 6AMLD, la police criminelle fédérale allemande a démantelé, le 19 septembre 2024, les infrastructures de 47 plateformes d'échange de crypto-actifs en russe ne procédant à aucune vérification d'identité (sans protocole KYC). Cette opération, baptisée « Opération Final Exchange », est d'une grande envergure et met en évidence le rôle crucial que jouent les plateformes d'*échange* instantané sans KYC dans la cybercriminalité (Menacho-Inga et al., 2025). Comme leur nom l'indique, ces sites sans protocole KYC ne disposent d'aucun processus visible permettant de recueillir les informations d'identification des utilisateurs avant de leur permettre de déposer ou de retirer des fonds, quel qu'en soit le montant. Ils ne demandent ni nom, ni numéro de téléphone, ni adresse e-mail, et ne prennent pas la peine de vérifier ces informations avant d'effectuer les transactions (Anggriawan & Susila, 2024).

L'une des principales vulnérabilités du cadre réglementaire actuel des crypto-actifs réside dans l'absence d'une autorité centrale capable de superviser et de contrôler les transactions. Confier la supervision et la réglementation des crypto-actifs à des agences non spécialisées réduit l'efficacité de ces réglementations. De même, sur le plan juridique, il n'existe ni lignes directrices ni conditions préalables pour l'obtention de licences permettant d'exercer des activités dans le domaine des crypto-actifs (Hope Kanu, 2025).

D'un point de vue comparatif, le modèle américain présente une approche fragmentée et réactive, fondée sur l'intervention a posteriori de différentes agences. En revanche, le modèle de l'UE se caractérise par une approche préventive et harmonisée, qui vise à réduire la pseudonymisation *ex ante*. Cependant, les deux systèmes présentent, au niveau de leur capacité opérationnelle, des limites pour faire face à la dimension internationale du phénomène.

Aucun des deux systèmes n'est pleinement efficace. Le modèle américain peut présenter des lacunes dans la phase préventive, tandis que le modèle européen continue de se heurter à des défis tant dans sa mise en œuvre effective que dans son adaptation à l'évolution technologique rapide de l'écosystème des cryptomonnaies.

8. NOUVEAUTÉS LÉGISLATIVES DE L'UNION EUROPÉENNE

[10] Il s'agit de l'acronyme de *« Markets in Crypto-Assets Regulation »*, le règlement (UE) 2023/1114 sur les marchés des crypto-actifs. Il s'agit de la première réglementation complète de l'UE régissant les crypto-actifs, leurs émetteurs et les prestataires de services qui y sont liés.

Les structures sociétaires opaques utilisées par les organisations criminelles pour blanchir des actifs virtuels : avec l'entrée en vigueur le 10 juillet 2027 d'une réglementation qui renforcera la transparence de la propriété effective, élargira la traçabilité et le contrôle des opérations sur les crypto-actifs, et interdira les comptes anonymes (règlement (UE) 2024/1624, art. 79, paragraphe 1) et exigera des mesures spécifiques pour les transferts vers des adresses auto-hébergées[11] (règlement (UE) 2024/1624, art. 40).

Parallèlement, le paquet législatif précédent a été actualisé par une nouvelle directive sur les mécanismes de prévention, qui instaure l'obligation pour les États membres de mettre en place des mécanismes permettant d'identifier la personne qui détient ou contrôle des comptes de crypto-actifs et d'interconnecter ces mécanismes via un système à l'échelle de l'UE (directive (UE) 2024/1640, art. 16). D'un point de vue juridique, la surveillance européenne est renforcée par la création de l'Autorité AMLA, qui est pleinement opérationnelle depuis le 1er juillet 2025 (Règlement (UE) 2024/1620).

8.1. QUELS CHANGEMENTS L'UE INTRODUIT-ELLE PAR RAPPORT AUX ÉTATS-UNIS POUR LUTTER CONTRE LE PSEUDONYMATISME ET L'OPACITÉ DANS L'UTILISATION DES CRYPTO-ACTIFS ?

L'UE interdit aux prestataires de services de crypto-actifs de tenir des comptes anonymes ou tout compte permettant de dissimuler l'identité du titulaire ou d'accroître l'opacité des transactions, en mentionnant spécifiquement les monnaies de confidentialité (règlement (UE) 2024/1624, art. 79, paragraphe 1). Conformément à cette approche, le paquet européen PBC/FT impose aux prestataires de services de crypto-actifs l'obligation d'identifier et d'évaluer les risques inhérents aux transferts vers des adresses auto-hébergées. De même, ces prestataires doivent mettre en œuvre des mesures d'atténuation proportionnées, pouvant aller jusqu'à l'identification et la vérification de l'expéditeur ou du destinataire, ainsi qu'à la collecte d'informations supplémentaires sur l'origine et la destination (règlement (UE) 2024/1624, art. 40, paragraphe 1). Ces règles renforcent l'objectif visant à limiter l'utilisation des crypto-actifs à des fins d'anonymisation, en particulier lorsqu'ils sont associés à des structures sociétaires opaques, un contexte que le cadre européen lui-même reconnaît comme générant des risques de contournement et de dissimulation et auquel répond le nouveau paquet législatif de 2024.

L'UE a préféré adopter le modèle de « tolérance zéro » vis-à-vis de la pseudonymisation, avec des interdictions directes, des règles uniformes et une nouvelle autorité supranationale. En revanche, les États-Unis suivent un modèle décentralisé où l'anonymat n'est pas interdit, et où les autorités agissent principalement par le biais de poursuites pénales ou administratives après avoir détecté des infractions.

La grande différence est simple. L'UE limite la pseudonymisation *ex ante* par des interdictions, tandis que les États-Unis la combattent *ex post* par *des mesures coercitives.*[12]

---

[11] Une adresse auto-hébergée est une adresse de cryptomonnaie contrôlée directement par un utilisateur, sans intervention ni conservation par un intermédiaire réglementé (tel qu'une plateforme d'échange ou un VASP).

[12] Il s'agit d'un terme anglo-saxon qui se traduit par « application », « exécution » ou « mise en œuvre de la loi ». Dans le domaine juridique et réglementaire, il désigne l'ensemble des actions, mesures et procédures mises en œuvre par les autorités compétentes pour garantir le respect effectif des règles. De manière générale, *l'« enforcement »* désigne la capacité et la pratique d'un État ou d'une autorité de régulation à enquêter, surveiller, sanctionner et corriger les manquements à la réglementation.

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

Tableau 1.
Différences clés entre l'UE et les États-Unis en matière de pseudonymisation et d'opacité des crypto-actifs.

DIMENSION	UE	États-Unis
Comptes anonymes.	Explicitement interdites (art. 79.1).	Non interdites par la loi fédérale.
Cryptomonnaies axées sur la confidentialité	Interdiction à partir de 2027.	Non interdites, mais soumises à une surveillance.
Portefeuille de crypto-actifs auto-hébergé.	Évaluation obligatoire des risques et identification possible (art. 40.1).	Il n'existe aucune obligation fédérale d'identification.
Cadre réglementaire.	Complet, unifié (MiCA + AMLR).	Fragmenté : SEC, CFTC, FinCEN, IRS, États.
Surveillance.	Centralisée en vertu de l'AMLA.	Décentralisée ; chaque agence agit dans son domaine de compétence.
Tokens privés.	Suppression totale.	Non interdits.
Approche.	Préventif, restrictif, traçabilité totale.	Réactif, sanctionnant, fondé sur *la mise en application de la réglementation.*

8.2. QUELLES SONT LES NOUVEAUTÉS CONCERNANT L'IDENTIFICATION DU PROPRIÉTAIRE RÉEL ET LA TRANSPARENCE DES SOCIÉTÉS FACE AUX STRUCTURES OPACES ?

Le règlement (UE) 2024/1624 précise la chaîne d'identification du bénéficiaire effectif en fonction de la propriété et du contrôle, et stipule que les informations relatives au bénéficiaire effectif doivent être adéquates, précises et à jour, et que les entités doivent informer le registre central sans retard injustifié et dans un délai maximal de 28 jours calendaires pour signaler tout changement (règlement (UE) 2024/1624, art. 63). Les informations requises pour obtenir les données relatives au bénéficiaire effectif sont élargies et précisées ; elles comprennent, entre autres, l'identification complète, la nature et l'étendue de l'intérêt réel et, en cas de structure comportant plusieurs entités ou instruments, la description de la structure de propriété et de contrôle (Règlement (UE) 2024/1624, art. 62). D'un point de vue juridique, la directive (UE) 2024/1640 établit des règles relatives à la création et à l'accès aux registres centraux des bénéficiaires effectifs et remplace la directive (UE) 2015/849, qui est abrogée à compter du 10 juillet 2027 (directive (UE) 2024/1640 ; effet abrogatoire).

Tout cela s'inscrit dans le cadre du renforcement du cadre de transparence et de coopération à l'échelle de l'UE, dans le but de limiter considérablement le recours à des sociétés écrans ou à des structures sociétaires opaques.

À l'inverse, les États-Unis facilitent le recours aux structures sociétaires en opérant un revirement à 180°, ce qui réduit considérablement la transparence : ils suppriment les

obligations pesant sur les entreprises américaines, affaiblissent le *Corporate Transparency Act*[13] et laissent la transparence à la discrétion des États.

Tableau 2.

Comparaison des cadres de transparence en matière de propriété effective et de surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme : Union européenne vs États-Unis.

ÉLÉMENT	UNION EUROPÉENNE	ÉTATS-UNIS
Chaîne d'identification du bénéficiaire effectif.	Détaillée, étendue et obligatoire (propriété + contrôle, étendue de la participation, structure sociétaire complète).	Presque entièrement supprimée pour les entités nationales à partir de 2025 ; ne s'applique qu'à certaines entités étrangères.[14]
Mise à jour des données.	Délai maximal de 28 jours calendaires pour notifier les changements.	Il n'existe aucune obligation fédérale pour les entreprises américaines.
Registres centraux.	Caractère obligatoire et harmonisation en vertu de la directive 2024/1640.	Il n'y a pas de registre fédéral pour les entités nationales après l'IFR de 2025 ; la transparence relève de la compétence des États. [15]
Stratégie face aux sociétés écrans.	Restrictive, préventive et fondée sur une traçabilité complète.	Assouplissement réglementaire : la disparition du système de déclaration fédéral facilite le recours à des structures sociétaires opaques.
Surveillance en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT).	Modèle européen unifié avec la loi AMLA.	*Application* fragmentée (FinCEN, IRS, SEC, CFTC), sans structure fédérale unique pour les bénéficiaires effectifs.

[13] Le *Corporate Transparency Act* (CTA) est une loi fédérale américaine, promulguée en 2021, dont l'objectif est de lutter contre le blanchiment d'argent, le financement du terrorisme, la fraude fiscale et l'utilisation de sociétés écrans en imposant l'obligation de déclarer des informations sur les bénéficiaires effectifs (*Beneficial Ownership Information*, BOI) de certaines entités.

[14] Financial Crimes Enforcement Network. (2025). *Beneficial Ownership Information Reporting. Département du Trésor des États-Unis*. 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). *Mise à jour sur la loi sur la transparence des entreprises (CTA) : état des lieux des obligations de déclaration des bénéficiaires effectifs au titre de la loi sur la transparence des entreprises et des initiatives connexes au 5 janvier 2026*. Pillsbury Winthrop Shaw Pittman LLP. https://www.pillsburylaw.com/en/news-and-insights/cta-update.html

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

8.3 IMPLICATIONS JURIDIQUES ET DOGMATIQUES DE L'IDENTIFICATION DU PROPRIÉTAIRE RÉEL

D'un point de vue dogmatique, le règlement (UE) 2024/1624 ne se limite pas à un simple renforcement de la transparence formelle, dans la mesure où il influe directement sur le développement structurel de la notion de propriété effective. Il permet ainsi de faire passer la priorité d'une perspective purement registrale à un principe matériel fondé sur une surveillance effective.

Du point de vue du droit pénal économique, ce changement est particulièrement important, car il réduit les marges d'imputation indéfinie propres aux structures sociétaires complexes. Lorsque l'identification du bénéficiaire effectif est requise en tenant compte à la fois de la propriété et du contrôle, le règlement établit un critère fonctionnel qui simplifie l'attribution juridique de la responsabilité. C'est notamment dans l' s infractions liées au blanchiment de capitaux que la dissimulation du bénéficiaire effectif constitue un élément constitutif central.

Dans ce même ordre d'idées, l'exigence selon laquelle les informations relatives à la propriété effective doivent être pertinentes, exactes et à jour, associée à l'obligation de notification dans un délai maximal de 28 jours (art. 63), ne revêt pas seulement un aspect administratif, mais a également des effets directs sur la force probante dans le cadre de la procédure pénale. À cet égard, les registres de propriété effective s'imposent comme de véritables outils d'analyse de *l'iter criminis* financier. Cette situation contribue à limiter les risques au stade de l'enquête et facilite la traçabilité juridique des fonds illicites.

L'élargissement du contenu informatif (art. 62), qui inclut la nature et l'étendue du droit réel ainsi que l'analyse des structures complexes, introduit quant à lui un aspect fondamental du point de vue de la doctrine du blanchiment. Cela permet d'établir un lien juridique entre la propriété économique et l'apparence formelle de légalité. Ce lien est essentiel pour contourner les limites conventionnelles du droit pénal face aux aspects de stratification et de ségrégation patrimoniale, éléments courants du blanchiment par le biais des crypto-actifs.

Conformément à cette approche, la directive (UE) 2024/1640 renforce la mise en place de systèmes d'accès et de centralisation des informations. Ainsi, elle établit une perspective qui va au-delà de la simple harmonisation normative en évoluant vers un cadre juridique de transparence au niveau supranational. Cette évolution implique une optimisation du principe de coopération administrative et judiciaire au sein de l'UE, principe essentiel dans un contexte de criminalité transnationale.

On peut affirmer que l'ensemble de ces règles crée les conditions nécessaires au maintien du modèle européen, en s'inscrivant dans une logique préventive et structurelle, visant non seulement à sanctionner les comportements, mais aussi à limiter *ex ante* les conditions de possibilité de l'infraction, en restreignant l'utilisation des entités juridiques comme mécanismes d'opacité.

Le modèle américain, en revanche, a des implications importantes pour la théorie du droit. Affaiblir le *Corporate Transparency Act* et assouplir les obligations d'identification du bénéficiaire effectif implique une évolution vers un système où

l'opacité sociétaire redevient un domaine de risque juridique significatif. D'un point de vue dogmatique, cela complique l'identification de l'auteur de l'infraction et rend plus difficile l'imputation pénale dans des structures complexes.

Cette position met en évidence une disparité structurelle entre les deux systèmes. D'une part, l'UE développe un modèle fondé sur l'identification *ex ante* et la traçabilité juridique. À l'inverse, les États-Unis conservent une logique majoritairement réactive, axée sur *l'application de la loi*, dans laquelle l'intervention intervient une fois que l'infraction a été commise.

D'un point de vue critique, cette divergence n'est pas seulement technique, mais reflète deux conceptions distinctes du droit pénal économique :

Un modèle européen de prévention structurelle et de réduction du risque systémique.

Un modèle américain de réaction punitive, de poursuite de l'infraction.

En réalité, l'évolution normative européenne témoigne d'un effort visant à résoudre la disparité traditionnelle entre traçabilité économique et imputation juridique. À l'inverse, le modèle américain continue de rencontrer des difficultés pour intégrer ces deux niveaux de manière cohérente dans le domaine de la criminalité économique.

8.4. COMMENT RENFORCER LES MÉCANISMES DE LOCALISATION DES COMPTES ET LA SURVEILLANCE EUROPÉENNE AFIN DE DÉTECTER LES SCHÉMAS IMPLIQUANT DES CRYPTO-ACTIFS ET LES ENTREPRISES AUX STRUCTURES OPAQUES ?

La directive (UE) 2024/1640 impose aux États membres de mettre en place des mécanismes automatisés centralisés permettant d'identifier en temps réel toute personne qui détient ou contrôle, entre autres, des comptes de crypto-actifs, ainsi que des comptes bancaires, des comptes de paiement, des comptes-titres et des coffres-forts (directive (UE) 2024/1640, art. 16, paragraphe 1).

Ces mécanismes doivent inclure des informations minimales sur le titulaire, le représentant, le bénéficiaire effectif ainsi que les dates d'ouverture et de clôture ; pour les comptes de crypto-actifs, ils doivent également comporter un identifiant unique et les dates d'ouverture et de clôture (directive (UE) 2024/1640, art. 16, paragraphe 3, point f). De même, leur interconnexion doit être prévue via le système BARIS[16] , que la Commission doit mettre en place et gérer, l'interconnexion devant être effective au plus tard le 10 juillet 2029 (directive (UE) 2024/1640, art. 16, paragraphe 6).

[16] Le *Bank Account Registers Interconnection System* (BARIS) est un système informatique à l'échelle européenne conçu pour interconnecter les registres nationaux des comptes bancaires des États membres de l'UE, permettant un accès rapide, sécurisé et harmonisé aux informations financières pertinentes pour la prévention, la détection, l'enquête et la poursuite des infractions graves, notamment le blanchiment d'argent et le financement du terrorisme.

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

Ce renforcement est complété par la création de l'AMLA[17] afin de superviser et d'harmoniser la surveillance, et de rendre plus efficace le système européen de prévention des risques transfrontaliers liés au blanchiment de capitaux et au financement du terrorisme (règlement (UE) 2024/1620 ; entrée en vigueur générale le 1er juillet 2025), dans le cadre du paquet législatif européen de 2024.

9. EFFICACITÉ DU CADRE RÉGLEMENTAIRE EN MATIÈRE DE BLANCHIMENT D'ARGENT PAR LE BIAIS DES CRYPTO-ACTIFS

La capacité à prévenir, détecter, attribuer la responsabilité et sanctionner le blanchiment de capitaux, considérée sous l'angle de l'efficacité réglementaire, nécessite un examen comparatif de ces cadres, dans la mesure où elle doit également être envisagée au regard des principes de légalité et de sécurité juridique. La définition des comportements typiques et leur enquête effective dépendent de la précision normative et de la capacité d'adaptation du droit pénal économique dans des environnements technologiques sophistiqués.

L'analyse de l'efficacité des cadres réglementaires en matière de BC par le biais des crypto-actifs doit aller au-delà d'une approche formelle centrée sur l'existence de normes. Son objectif est d'évaluer leur capacité réelle à prévenir, détecter et poursuivre les comportements illicites dans un environnement technologiquement sophistiqué, ainsi que la dimension internationale de ce phénomène. Le degré de développement réglementaire doit également être examiné à l'aune de son fonctionnement pratique et de sa capacité d'adaptation aux dynamiques de l'écosystème des cryptomonnaies.

Il est possible, à partir de ce postulat, d'identifier des critères juridiques et opérationnels permettant d'évaluer l'efficacité des systèmes de lutte contre le blanchiment de capitaux dans ce domaine.

9.1. CAPACITÉ DE PRÉVENTION

Pour qu'un système soit efficace en matière de politiques de prévention et de répression du blanchiment de capitaux, le premier pilier est la prévention. Ce premier pilier se concrétise principalement, dans le domaine des crypto-actifs, par les obligations de diligence prévues à l'article 13 de la directive (UE) 2015/849, relatives à la connaissance du client (KYC) et à l'évaluation des risques, auxquelles les prestataires de services d'actifs virtuels (VASP) doivent se conformer.

Le modèle de l'UE présente une approche plus solide, un système harmonisé assorti d'obligations clairement définies pour les intermédiaires, renforçant la traçabilité et limitant le pseudonymat. Le modèle américain, en revanche, se heurte à de nombreuses contraintes opérationnelles pour établir des obligations uniformes, ce qui pourrait créer des zones de risque.

[17] L'AMLA (*Anti-Money Laundering Authority* / Autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme) est une agence décentralisée de l'UE, créée en 2024 et dont le siège est à Francfort, dont l'objectif est de superviser, coordonner et renforcer le respect des règles européennes en matière de prévention du blanchiment de capitaux (AML) et du financement du terrorisme (CFT).

Toutefois, l'efficacité préventive ne dépend pas uniquement de l'existence de ces obligations, mais aussi d'une mise en œuvre et d'une surveillance adéquates.

9.2. CAPACITÉ DE DÉTECTION

La détection des opérations suspectes est cruciale pour lutter contre le blanchiment d'argent. Dans le domaine des monnaies numériques, cette capacité se traduit par l'utilisation d'outils d'analyse de *la blockchain* et par la collaboration entre acteurs publics et privés.

La traçabilité ou le suivi technique de ces opérations sur les réseaux publics ne permet pas toujours d'identifier effectivement les participants impliqués. L'efficacité des réglementations repose sur le renforcement des capacités techniques des autorités et sur la collaboration avec des organismes spécialisés.

9.3. CAPACITÉ D'ATTRIBUTION

Comme mentionné dans l'analyse de la propriété effective, le renforcement des systèmes d'identification prévus par le règlement (UE) 2024/1624 contribue à combler le fossé classique entre la traçabilité technique et l'attribution juridique. Dans le cadre de la criminalité organisée impliquant des crypto-actifs, l'un des principaux défis structurels réside dans la séparation entre la traçabilité des transactions et l'attribution juridique à des personnes physiques ou morales spécifiques.

Ainsi, l'exigence d'informations précises, actualisées et fonctionnellement complètes sur le bénéficiaire effectif permet d'identifier des points de connexion entre les transactions enregistrées dans des systèmes décentralisés. La *blockchain*, par exemple , et certaines entités juridiques en sont un exemple, car elles facilitent ainsi l'imputation pénale dans les cas de criminalité liée aux cryptomonnaies.

D'un point de vue dogmatique, ces mécanismes renforcent la possibilité d'identifier le véritable titulaire économique au-delà des constructions formelles, ce qui revêt une importance capitale pour la constitution de l'élément subjectif de l'infraction et pour la preuve de la connaissance de l'origine illicite des fonds. Ainsi, l'architecture réglementaire européenne renforce non seulement la capacité de détection, mais influe également de manière décisive sur la capacité d'imputation juridique, comblant ainsi l'une des principales lacunes structurelles du système traditionnel face aux nouvelles formes de criminalité financière basées sur les crypto-actifs.

Il est nécessaire de prouver l'existence d'opérations suspectes pour qu'une enquête soit ouverte sur une infraction, ainsi que leur lien avec un sujet donné et la connaissance de l'origine illicite des fonds. Les réseaux *blockchain*, associés à l'utilisation de *mixeurs*, de cryptomonnaies axées sur la confidentialité ou de structures de stratification, compliquent cette tâche en raison de leur nature pseudonyme.

L'efficacité des cadres réglementaires dépend de leur capacité à créer des points de connexion entre le domaine numérique et le monde juridique grâce à des mécanismes d'identification et à des obligations d'information.

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

9.4. CAPACITÉ D'EXÉCUTION ET DE SANCTION

Le dernier élément d'évaluation porte sur la capacité à enquêter, à sanctionner et à confisquer les avoirs illicites. Cette dimension présente des caractéristiques propres au domaine des crypto-actifs, telles que *la blockchain*, les transferts transfrontaliers et les contraintes opérationnelles et techniques liées à leur confiscation.

L'approche fondée sur *l'application de la loi*, conforme au modèle américain, se caractérise par une forte capacité d'enquête et de poursuites pénales. Ce caractère réactif peut toutefois s'avérer insuffisant s'il n'est pas complété par des mesures préventives.

À l'inverse, on observe un renforcement de l'UE dans ses instruments de surveillance grâce à la création de l'AMLA, dont l'efficacité dépend de sa capacité à coordonner les autorités nationales.

9.5. ÉVALUATION COMPARATIVE DE L'EFFICACITÉ

Après analyse, ce critère nous montre qu'aucun des modèles, pris isolément, n'est pleinement efficace. Le système américain présente des atouts en matière de sanctions, mais des lacunes en matière de prévention structurelle. En revanche, le modèle de l'UE offre un cadre plus cohérent et préventif, même s'il se heurte à un défi structurel dans sa mise en œuvre.

Pour garantir l'efficacité des cadres réglementaires au-delà du simple développement normatif, il est nécessaire que la réglementation, les capacités technologiques, la coopération internationale et la spécialisation institutionnelle interagissent. La séparation entre l' e la planification normative et la capacité opérationnelle constitue le principal problème, ce qui renforce la nécessité d'une approche globale et coordonnée.

La nécessité d'une évolution du droit pénal économique met en évidence la nécessité de concilier l'efficacité des enquêtes et le respect des garanties fondamentales.

10. CONCLUSIONS

L'analyse développée tout au long de ce travail permet de confirmer que l'efficacité des cadres réglementaires en matière de BC par le biais des crypto-actifs ne dépend pas uniquement de leur degré de développement normatif. En ce sens, elle dépend de leur capacité réelle à prévenir, détecter, attribuer la responsabilité et sanctionner les comportements illicites, en créant les conditions permettant d'affirmer que les crypto-actifs, les cryptomonnaies et les actifs virtuels donnent lieu à des méthodes singulières, grâce à leur pseudonymat et à la nature mondiale et décentralisée de la technologie *blockchain*, un phénomène en pleine expansion. Les organisations criminelles exploitent délibérément ces caractéristiques, en recourant à une combinaison de techniques sophistiquées de dissimulation (par exemple, *le « smurfing »*, les portefeuilles de crypto-actifs, les services de mixage, les monnaies privées, les ponts entre *blockchains*) et de

structures d'entreprise opaques.[18] Cela permet de fragmenter, de déplacer et de dissimuler la trace des fonds, des transactions et des services de mixage, des monnaies privées et des ponts, autant d'outils susceptibles d'être exploités illicitement pour rendre leurs traces encore plus opaques. Cette combinaison technologique et sociétaire démontre que l'utilisation illicite de ces environnements n'est pas fortuite, mais stratégique et délibérée. Les marchés du *darknet* jouent toutefois un rôle de facilitateurs dans ces cas, puisqu'ils offrent des espaces propices au commerce anonyme.

D'après l'analyse réalisée, on peut affirmer que le blanchiment d'argent via les crypto-actifs est un phénomène complexe. Il se caractérise par l'interaction entre l'infrastructure technologique de l'écosystème numérique, la dimension internationale des opérations et la capacité d'adaptation des organisations criminelles. L'existence de cadres réglementaires à cet égard ne suffit pas à garantir leur efficacité.

Les États-Unis et l'Union européenne mettent en évidence des approches très différentes en ce qui concerne l'étude de leurs modèles réglementaires. Alors que le modèle américain repose sur une approche axée sur *l'application de la loi*, les capacités d'enquête et de sanction, l'Union européenne a, quant à elle, développé un système plus harmonisé et préventif, visant à limiter le pseudonymat et à renforcer la traçabilité des transactions. Ces deux modèles, qu'il s'agisse de la prévention structurelle ou de l'application concrète des règles, présentent des limites évidentes.

La traçabilité technique des transactions, comme cela a été souligné, ne se traduit pas toujours par une identification effective des personnes impliquées, ce qui engendre des défis probatoires majeurs et limite l'imputation juridique de l'infraction. C'est pourquoi l'efficacité du cadre réglementaire ne peut être mesurée uniquement à l'aune du degré de développement normatif. Elle doit être évaluée à l'aune de la capacité réelle de prévention, de détection, d'imputation et de sanction des comportements illicites.

L'idée selon laquelle l'efficacité dépend de l'intégration de mécanismes de surveillance, de capacités techniques et de coopération internationale corrobore cette réalité. L'utilisation de portefeuilles de crypto-actifs appartenant à des tiers, de services de *« mixing »*, de monnaies axées sur la confidentialité ou des marchés du *darknet et du deep web* montre que le problème ne réside pas uniquement dans le pseudonymat, mais dans la combinaison de facteurs technologiques, réglementaires et institutionnels.

L'effort institutionnel visant à lutter contre le blanchiment d'argent via les crypto-actifs nécessite une approche globale combinant réglementation, technologie et capacités opérationnelles, afin de combler le fossé entre la conception normative et son application effective. Cette interaction permet de renforcer la prévention, la détection et la poursuite dans le domaine des crypto-actifs, dans la mesure où aucun des modèles examinés ne s'avère pleinement efficace à lui seul.

[18] Une société opaque est une entité juridique dont la structure de propriété, de contrôle et de bénéficiaires effectifs est conçue pour dissimuler l'identité des personnes qui possèdent ou contrôlent réellement l'entreprise. Sa caractéristique essentielle est le manque de transparence, qui empêche d'identifier le bénéficiaire effectif (*ultimate beneficial owner*, UBO).

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

La principale contribution de cette étude réside dans l'identification du décalage entre la traçabilité technologique et l'imputation juridique comme axe central des limites actuelles du système de prévention du BC dans le domaine des crypto-actifs.

11. RÉFLEXION FINALE

L'étude du blanchiment d'argent par le biais des crypto-actifs met en évidence un phénomène qui dépasse les catégories traditionnelles du droit pénal et de la réglementation financière. L'évolution technologique a non seulement apporté des possibilités d'innovation et de nouvelles formes de circulation de la valeur, mais elle ouvre également la voie à la création d'espaces de risque difficiles à intégrer dans les modèles réglementaires existants.

Cette étude comparative montre clairement que ni une approche axée sur la *répression*, ni un modèle à dominante préventive ne suffisent à eux seuls, car il devient nécessaire de repenser les mécanismes conventionnels d'intervention juridique. La capacité des systèmes juridiques à s'adapter à un environnement marqué par la rapidité, la décentralisation et la complexité technique constitue le nouveau défi auquel nous sommes contraints de faire face, tout comme la nécessité de réglementations plus modernes.

Dans le contexte des crypto-actifs, qui reflète une tension croissante entre traçabilité technique et attribution juridique, entre réglementation formelle et efficacité opérationnelle, la Banque centrale va au-delà des divergences entre juridictions. Le nouveau rôle des institutions oblige à repenser cette tension, la coopération internationale et l'intégration des capacités technologiques en tant qu'éléments essentiels du système.

La réponse institutionnelle définitive pour atténuer ce phénomène ne peut être uniquement normative, mais doit également être technologique. Une approche globale permettra de réduire l'écart entre l'élaboration des normes et leur mise en œuvre efficace, garantissant ainsi une réponse juridique cohérente face à un phénomène en constante évolution.

12. RÉFÉRENCES BIBLIOGRAPHIQUES

Anggriawan, R., & Susila, M. (2024). La cryptomonnaie et ses liens avec le blanchiment d'argent et le financement du terrorisme dans le cadre des recommandations du GAFI. *Novum Jus, 18(2)*. Disponible sur : https://doi.org/10.14718/novumjus.2024.18.2.10 [Dernière consultation : 23/02/2026].

Akkoyun, A. G., & Çelik, M. E. (2022). La criminalité organisée transnationale et la Convention des Nations unies. *Frontiers in Law, 1, 9–21*. Disponible sur : https://doi.org/10.6000/2817-2302.2022.01.02 [Dernière consultation : 23/02/2026].

Alessi Longa, F. (2025). Cryptomonnaies et blanchiment d'argent. *American Journal of Industrial and Business Management, 15(2), 362–371*. Disponible à l'adresse : https://doi.org/10.4236/ajibm.2025.152017 [Dernière consultation : 23/02/2026].

Anguren, R., García Alcorta, J., García Calvo, L., Hernández García, D., & Valdeolivas, E. (2023). La réglementation des crypto-actifs dans le cadre international et européen actuel. *Revue de stabilité financière*, 44, Banque d'Espagne. Disponible sur : https://doi.org/10.53479/30054 [Dernière consultation : 23/02/2026].

Arnone, G., Scirè, G., & Bivona, E. (2025). L'utilisation (abusive) des cryptomonnaies par les organisations criminelles : une revue systématique de la littérature. *Digital Finance, 7, 815–851*. Disponible sur : https://doi.org/10.1007/s42521-025-00148-1 [Dernière consultation : 23/02/2026].

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). La criminalistique de la blockchain : une revue systématique de la littérature. *Electronics, 13(17), 3568*. Disponible sur : https://doi.org/10.3390/electronics13173568 [Dernière consultation : 23/02/2026].

Baer, K., de Mooij, R., Hebous, S., & Keen, M. (2023). Taxation des cryptomonnaies. *Oxford Review of Economic Policy, 39(3), 478–497*. Disponible à l'adresse : https://doi.org/10.1093/oxrep/grad035 [Dernière consultation : 23/02/2026].

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

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

Blanco Barón, C. (2025). La réglementation des crypto-actifs : au-delà d'un problème d'efficacité. *Revue d'économie institutionnelle, 27(53), 133–186*. Disponible sur : https://doi.org/10.18601/01245996.v27n53.07 [Dernière consultation : 23/02/2026].

Chiang, S. (2024). Les cryptomonnaies sont de plus en plus utilisées à des fins de blanchiment d'argent. CNBC. Disponible sur : https://www.cnbc.com/2024/07/16/crypto-is-increasingly-being-used-for-money-laundering-chainalysis-says.html [Dernière consultation : 23/02/2026].

Cremers, C., Loss, J., & Wagner, B. (2024). Une analyse holistique de la sécurité des transactions Monero. Dans Advances in Cryptology – EUROCRYPT 2024 (pp. 129–159). *Springer*. Disponible à l'adresse : https://doi.org/10.1007/978-3-031-58734-4_5 [Dernière consultation : 23/02/2026].

Enríquez Pérez, I. (2020). Le crime organisé et la fragilité institutionnelle en tant que facteurs déterminants du développement. *Revue de la Faculté des sciences économiques*, 28(1). Disponible sur : https://doi.org/10.18359/rfce.3564 [Dernière consultation : 23/02/2026].

Farrukh, H., Zafar, S., Rehman, Z. U., Shah, A. A., & Alshammry, N. (2025). Détection des fraudes basée sur la blockchain : revue systématique comparative de la littérature sur les approches d'apprentissage fédéré et d'apprentissage automatique. *Electronics*, 14(24), 4952. Disponible sur : https://doi.org/10.3390/electronics14244952 [Dernière consultation : 23/02/2026].

Fu, Q., Liu, J., Pan, S., & Yuen, T. H. (2025). SoK : une analyse approfondie des techniques de lutte contre le blanchiment d'argent pour les cryptomonnaies sur blockchain. *Dans ACISP 2025*. Disponible sur : https://doi.org/10.1007/978-981-96-9095-4_16 [Dernière consultation : 23/02/2026].

Gorjón, S. (2023). La finance décentralisée ou les crypto-actifs de nouvelle génération. *Bulletin économique 2023/T3*, art. 04. Disponible sur : https://doi.org/10.53479/30650 [Dernière consultation : 23/02/2026].

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

Hinojal, A. (2023). Cryptomonnaies et blanchiment d'argent. *Logos Guardia Civil, 1, 215–240*. Disponible sur : revistacugc.es/article/view/5742 [Dernière consultation : 23/02/2026].

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

Hope Kanu, D. (2025). La réglementation des cryptomonnaies et ses implications pour la stabilité financière : une analyse qualitative. *IJEBMR, 9(4)*. Disponible sur : https://doi.org/10.51505/IJEBMR.2025.9416 [Dernière consultation : 23/02/2026].

Isolauri, E. A., & Ameer, I. (2023). Le blanchiment d'argent en tant que phénomène commercial transnational : une revue systématique et un programme pour l'avenir. *Critical Perspectives on International Business, 19(3), 426–468*. Disponible à l'adresse : https://doi.org/10.1108/cpoib-10-2021-0088 [Dernière consultation : 23/02/2026].

Jordá, C., Píriz, C., & Giménez-Salinas, A. (2024). Les marchés illicites de trafic de drogue sur le Dark Web : une étude empirique exploratoire. *Revista Española de Investigación Criminológica, 22(2)*. Disponible sur : https://doi.org/10.46381/reic.v22i2.884 [Dernière consultation : 23/02/2026].

Kabra, S., & Gori, S. (2025). Lutter contre le blanchiment de cryptomonnaies par les groupes criminels organisés grâce à un cadre réglementaire efficace. *IIUM Law*

Journal, 33(1). Disponible sur : https://doi.org/10.31436/iiumlj.v33i1.1007 [Dernière consultation : 23/02/2026].

Koelbing, M., Kieseberg, K., Çulha, C., Garn, B., & Simos, D. E. (2024). Modélisation des schémas de « smurfing » dans les cryptomonnaies à l'aide de partitions d'entiers. *IET Blockchain*. Disponible à l'adresse : https://doi.org/10.1049/blc2.12087 [Dernière consultation : 23/02/2026].

Langdale, J. (2024). Lutte contre le blanchiment d'argent dans les casinos d'Asie du Sud-Est et d'Australie. Dans Financial Crime and the Law (pp. 225–245). *Springer*. Disponible sur : https://doi.org/10.1007/978-3-031-59543-1_9 [Dernière consultation : 23/02/2026].

Legrand, T., & Leuprecht, C. (2021). Renforcer la collaboration transfrontalière : les réseaux transgouvernementaux de lutte contre la criminalité. *Policy and Society*, 40(4), 565–586. Disponible à l'adresse : https://doi.org/10.1080/14494035.2021.1975216 [Dernière consultation : 23/02/2026].

Lim, A., & Choi, K.-S. (2025). Modus operandi et analyse blockchain des escroqueries sentimentales : victimisation liée aux cryptomonnaies. *International Journal of Cybersecurity Intelligence & Cybercrime, 8(2)*. Disponible à l'adresse : https://doi.org/10.52306/2578-3289.1220 [Dernière consultation : 23/02/2026].

Lom, A., & Hashmall, R. (2021). *Publication des nouvelles lignes directrices du GAFI sur les actifs virtuels et les prestataires de services d'actifs virtuels (VASP)*. Disponible sur : https://www.nortonrosefulbright.com/en-us/knowledge/publications/024b3d80/new-fatf-guidance-released-on-virtual-assets-and-virtual-asset-service-providers [Dernière consultation : 23/02/2026].

Luna Galván, M., Luong, H. T., & Astolfi, E. (2021). Le trafic de drogue en tant que crime organisé : une perspective transnationale et multidimensionnelle. *Revue des relations internationales, de la stratégie et de la sécurité, 16(1)*. Disponible sur : https://doi.org/10.18359/ries.5412 [Dernière consultation : 23/02/2026].

Medranda Morales, N., & Arcos Argudo, M. (2023). Crypto-actifs et cryptomonnaies. Dans Blockchain, crypto-actifs et métaverse (pp. 41–62). *Éditions Abya-Yala*. Disponible sur : https://doi.org/10.17163/abyaups.6 [Dernière consultation : 23/02/2026].

Menacho-Inga, W. G., Proaño-Reyes, G., & Castro-Sánchez, F. (2025). L'utilisation des cryptomonnaies et le blanchiment d'argent en Équateur. *Noesis, 7(esp2)*. Disponible sur : https://doi.org/10.35381/noesisin.v7i2.620 [Dernière consultation : 23/02/2026].

Mollaahmetoğlu, M. B., & Baykut, C. (2021). *Lignes directrices actualisées du Groupe d'action financière*. Disponible sur : https://chambers.com/articles/financial-action-task-force-s-updated-guidance-virtual-assets-and-virtual-asset-service-providers [Dernière consultation : 23/02/2026].

Montoya Arrubla, E. (2025). *Mécanismes de contrôle du blanchiment des crypto-actifs*. Diálogos Punitivos. Disponible sur : https://dialogospunitivos.com/wp-content/uploads/2025/04/Columna-de-interes-43.pdf [Dernière consultation : 23/02/2026].

Rodríguez-Valencia, L., et al. (2025). Une revue systématique de l'intelligence artificielle appliquée à la conformité : détection de la fraude dans les transactions en cryptomonnaies. *Journal of Risk and Financial Management, 18(11), 612*. Disponible à l'adresse : https://doi.org/10.3390/jrfm18110612 [Dernière consultation : 23/02/2026].

Soltani, R., Zaman, M., Joshi, R., & Sampalli, S. (2022). Technologies des registres distribués et leurs applications : une revue. *Applied Sciences, 12(15), 7898*. Disponible sur : https://doi.org/10.3390/app12157898 [Dernière consultation : 23/02/2026].

Sudan, H. K., Tai, A. M. Y., Kim, J., & Krausz, R. (2023). Décrypter les marchés des cryptomonnaies. Drug Science, *Policy and Law, 9, 1–19*. Disponible à l'adresse : https://doi.org/10.1177/20503245231215668 [Dernière consultation : 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). Actifs numériques : risques, réglementations, mesures d'atténuation. *Financial Innovation, 12, 65*. Disponible sur : https://doi.org/10.1186/s40854-025-00848-y [Dernière consultation : 23/02/2026].

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptomonnaies et criminalité financière future. *Crime Science, 11(1)*. Disponible sur : https://doi.org/10.1186/s40163-021-00163-8 [Dernière consultation : 23/02/2026].

Wang, H.-M., & Hsieh, M.-L. (2023). Les cryptomonnaies sont à la mode : réflexion sur la prévention du blanchiment d'argent. *Security Journal, 37, 25–46*. Disponible à l'adresse : https://doi.org/10.1057/s41284-023-00366-5 [Dernière consultation : 23/02/2026].

Warren, E., & Marshall, R. (2022). *Loi de 2022 sur la lutte contre le blanchiment d'argent lié aux actifs numériques (S.5267)*. Sénat des États-Unis. Disponible sur : https://www.congress.gov/bill/117th-congress/senate-bill/5267 [Dernière consultation : 23/02/2026].

13. RAPPORTS D'ORGANISMES

AMLC. (2023). *Analyse des transactions suspectes liées aux « junkets » de casino.* Disponible sur : http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf [Dernière consultation : 23/02/2026].

DEA. (2025). *Évaluation nationale de la menace liée à la drogue 2025*. Disponible sur : https://www.dea.gov/documents/2025/2025-05/2025-05-13/national-drug-threat-assessment [Dernière consultation : 23/02/2026].

Europol. (2024). *Cryptomonnaies – Suivi de l'évolution des finances criminelles.* Disponible sur : https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [Dernière consultation : 23/02/2026].

Europol. (2022). Cryptomonnaies : retracer l'évolution des finances criminelles. *Série « Spotlight » d'Europol*. Disponible à l'adresse : https://doi.org/10.2813/75468 [Dernière consultation : 23/02/2026].

GAFI, Groupe Egmont, INTERPOL et ONUDC. (2025). *Coopération internationale en matière de détection, d'enquête et de poursuites relatives au blanchiment d'argent : manuel*. Paris : GAFI. Disponible à l'adresse : https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html [Dernière consultation : 23/02/2026].

GAFI. (2024). *Actifs virtuels : normes du GAFI et mise en œuvre.* GAFI. Disponible sur : https://www.fatf-gafi.org/en/topics/virtual-assets.html [Dernière consultation : 23/02/2026].

GAFI. (2023). *Mise à jour ciblée sur la mise en œuvre des normes du GAFI relatives aux actifs virtuels et aux prestataires de services d'actifs virtuels (VASP).* GAFI. Disponible à l'adresse : https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [Dernière consultation : 23/02/2026].

GAFI.1. (2023). *Actifs virtuels :* normes *mondiales* du GAFI. Disponible sur : https://www.fatf-gafi.org/en/topics/virtual-assets.html [Dernière consultation : 23/02/2026].

GAFI. (2022). *Blanchiment d'argent lié au fentanyl et aux opioïdes de synthèse.* Disponible à l'adresse : https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.coredownload.inline.pdf [Dernière consultation : 23/02/2026].

GAFI. (2021). *Lignes directrices actualisées pour une approche fondée sur les risques concernant les actifs virtuels et les prestataires de services d'actifs virtuels*

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

(VASP). Disponible à l'adresse : https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf [Dernière consultation : 23/02/2026].

FinCEN. (2025). *Avis sur les réseaux chinois de blanchiment d'argent*. Disponible sur : https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering [Dernière consultation : 23/02/2026].

Ministère de l'Intérieur. (15 novembre 2024). *Opération conjointe de la Police nationale et de la Nationale Politie des Pays-Bas (méthode OTC)*. Disponible sur : https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16371# [Dernière consultation : 23/02/2026].

NYDFS. Département des services financiers de l'État de New York. (2024–2026). *Agrément des entreprises de monnaies virtuelles.* Disponible sur : https://www.dfs.ny.gov/virtual_currency_businesses [Dernière consultation : 23/02/2026].

ONUDC. (2026). *Programme mondial sur la cybercriminalité (supports de renforcement des capacités)*. Capacités/formation sur les cryptomonnaies/le darknet/les preuves numériques : Disponible sur : https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/capacitybuilding.html. Catalogue de formation 2024 : https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf [Dernière consultation : 23/02/2026].

ONUDC. (2025). *Point d'inflexion : implications mondiales des centres d'escroquerie, du système bancaire clandestin et des marchés illicites en ligne.* Disponible à l'adresse : https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html [Dernière consultation : 23/02/2026].

ONUDC. (2024). *Rapport annuel 2024 : Section sur la criminalité organisée. Office des Nations Unies contre la drogue et le crime.* Disponible sur : https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Dernière consultation : 23/02/2026].

ONUDC.1. (2024). *Réseaux criminels et structures fragmentées.* Disponible sur : https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Dernière consultation : 23/02/2026].

UNODC.2. (2024). *Casinos, blanchiment d'argent, système bancaire clandestin et criminalité organisée transnationale en Asie de l'Est et du Sud-Est : une menace cachée et croissante*. Disponible sur : https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf [Dernière consultation : 23/02/2026].

Ministère américain de la Justice. (2023). *États-Unis c. Binance Holdings Limited, opérant sous le nom de Binance.com (présentation de l'affaire).* Disponible à

l'adresse : https://www.justice.gov/criminal/case/united-states-v-binance-holdings-limited-dba-binancecom [Dernière consultation : 23/02/2026].

Ministère américain de la Justice.1. (2023). *États-Unis c. Changpeng Zhao (présentation de l'affaire)*. Disponible sur : https://www.justice.gov/criminal/case/united-states-v-changpeng-zhao [Dernière consultation : 23/02/2026].

14. LÉGISLATION

Conseil de l'Union européenne. (2024) Directive (UE) 2024/1640 du Parlement européen et du Conseil du 31 mai 2024 relative aux mécanismes que les États membres doivent mettre en place afin de prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant la directive (UE) 2019/1937 et modifiant et abrogeant la directive (UE) 2015/849. JOUE L 2024/1640 du 19 juin 2024.

Organisation des Nations unies. (2000). Nations unies. (2000). Convention des Nations unies contre la criminalité transnationale organisée (Résolution A/RES/55/25).

Parlement européen. (2024). Sixième directive anti-blanchiment. Résolution législative du Parlement européen du 24 avril 2024 sur la proposition de directive relative aux mesures visant à prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et abrogeant la directive (UE) 2015/849. JOUE C/2025/3790, 17 septembre 2025.

Parlement européen et Conseil de l'Union. (2024) Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. JOUE L 2024/1624, 19 juin 2024.

Parlement européen et Conseil de l'Union. (2024) Règlement (UE) 2024/1620 du Parlement européen et du Conseil du 31 mai 2024, portant création de l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme et modifiant les règlements (UE) n° 1093/2010, (UE) n° 1094/2010 et (UE) n° 1095/2010. JOUE L 2024/1620, 19 juin 2024

Parlement européen et Conseil de l'Union. (2023) Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 relatif aux informations accompagnant les transferts de fonds et de certains crypto-actifs et modifiant la directive (UE) 2015/849. JOUE, L 150, 9 juin 2023.

Congrès des États-Unis. (1977). Loi sur les pouvoirs économiques d'urgence internationaux (International Emergency Economic Powers Act), Pub. L. n° 95-223, 91 Stat. 1625–1629 (codifiée telle que modifiée aux articles 1701 à 1707 du titre 50 du Code des États-Unis).

Congrès des États-Unis. (1970). Loi sur le secret bancaire, Pub. L. n° 91-508, 84 Stat. 1114

(codifiée telle que modifiée aux articles 5311 à 5336 du titre 31 du Code des États-Unis).

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

15. AUTRES SOURCES NON SCIENTIFIQUES

Binance Academy. (2024). Qu'est-ce que le minage de cryptomonnaies et comment fonctionne-t-il ? Binance. Disponible sur : https://www.binance.com/es/academy/articles/what-is-crypto-mining-and-how-does-it-work [Dernière consultation : 23/02/2026].

Chainalysis. (2025). Tendances 2025 en matière de criminalité liée aux cryptomonnaies : les volumes illicites laissent présager une année record alors que la criminalité sur la chaîne devient de plus en plus diversifiée et professionnalisée. Disponible sur : https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ [Dernière consultation : 23/02/2026].

Équipe éditoriale de Coinmetro. (2 août 2024). Crypto Mixers : outils de confidentialité et défis réglementaires. *Coinmetro*. Disponible sur : https://coinmetro.com/learning-lab/crypto-mixers-privacy-tools-and-regulatory-challenges [Dernière consultation : 23/02/2026].

Elliptic. (2024). *Prévenir la criminalité financière dans le domaine des crypto-actifs : rapport sur les typologies*. https://www.elliptic.co/hubfs/Elliptic%20Typologies%20Report%202024.pdf [Dernière consultation : 23/02/2026].

16. DÉCLARATION D'INTÉGRITÉ ACADÉMIQUE ET SCIENTIFIQUE

Le présent travail est un travail original, réalisé par moi-même, sans plagiat ni utilisation abusive d'œuvres d'autrui, conformément aux normes internationales d'intégrité académique et scientifique.

Les données, les résultats et les conclusions ont été obtenus et traités de manière honnête et rigoureuse, sans fabrication, falsification ni manipulation abusive.

L'utilisation de l'intelligence artificielle ou d'autres outils numériques s'est conformée à la réglementation universitaire, sans se substituer à la paternité intellectuelle ni à mon propre jugement académique.

Il n'existe aucun conflit d'intérêts ayant influencé le déroulement ou les résultats de la recherche.

Je suis conscient que le non-respect de ces déclarations peut entraîner l'annulation du titre de docteur ainsi que les responsabilités académiques ou juridiques qui en découlent.

Par la présente, J'ASSUME toute responsabilité découlant du non-respect de l'engagement éthique énoncé dans la présente déclaration.