Faculté de droit
de sciences politiques et de gestion
Université de Strasbourg

Master 2 Droit des affaires

Juriste conformité / Compliance Officer (JCCO)

Année universitaire 2025-2026

LA RÉGULATION DES CRYPTO-ACTIFS PAR L'ENCADREMENT DES INTERMÉDIAIRES : LA PLACE DE L'ÉTABLISSEMENT BANCAIRE DANS LE DISPOSITIF EUROPÉEN DE PRÉVENTION DU BLANCHIMENT

Mémoire présenté et soutenu par :
Najwa BARKAN
Le 7 septembre 2026

Mémoire dirigé par :
Monsieur Doreid BECHERAOUI
Maître de conférences, Université de Strasbourg

REMERCIEMENTS

Je tiens à exprimer ma reconnaissance à Monsieur Doreid Becheraoui, qui a dirigé ce mémoire. Ses conseils, sa disponibilité et la rigueur de ses observations ont orienté ce travail à chacune de ses étapes.

Mes remerciements vont également à Madame Florence Thépot, directrice du Master 2 Juriste conformité, pour son dévouement et pour l'accompagnement constant dont elle entoure les étudiants de la promotion.

Je remercie Monsieur Aldric Valleteau de Moulliac, responsable de l'équipe Supervision AML-CTF, pour son accompagnement tout au long de cette année d'alternance et pour la confiance qu'il m'a accordée. Cette expérience a nourri la perspective pratique adoptée dans le présent mémoire.

Ma gratitude s'adresse enfin à Monsieur Gaëtan Fleury, dont l'expertise en matière de crypto-actifs, la disponibilité et les précieux conseils ont éclairé les développements les plus techniques de ce travail.

Que soient également remerciées les personnes qui ont accepté de relire ce mémoire et dont les remarques en ont amélioré la clarté.

SOMMAIRE

INTRODUCTION

CHAPITRE 1 — LA RÉGULATION PAR LES INTERMÉDIAIRES, TECHNIQUE FONDATRICE DU DISPOSITIF EUROPÉEN

Section 1 — Le choix de l'intermédiation comme technique de prévention

Section 2 — Les angles morts de l'intermédiation

CHAPITRE 2 — L'ÉTABLISSEMENT BANCAIRE, DÉBITEUR D'UNE VIGILANCE SANS RÉFÉRENTIEL CONSTITUÉ

Section 1 — Une vigilance construite sur une information exogène

Section 2 — Une obligation mesurée à un standard indéterminé

CONCLUSION GÉNÉRALE

BIBLIOGRAPHIE

TABLE DES MATIÈRES

LISTE DES ACRONYMES

ABE : Autorité bancaire européenne (*European Banking Authority*, EBA)

ACPR : Autorité de contrôle prudentiel et de résolution

AEMF : Autorité européenne des marchés financiers (*European Securities and Markets Authority*, ESMA)

ALBC : Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme (*Anti-Money Laundering Authority*, AMLA)

AMF : Autorité des marchés financiers

AMLR : Règlement (UE) 2024/1624 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme

BC-FT : Blanchiment de capitaux et financement du terrorisme

CJUE : Cour de justice de l'Union européenne

C. mon. fin. : Code monétaire et financier

COLB : Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme

DeFi : Finance décentralisée (*decentralised finance*)

GAFI : Groupe d'action financière (*Financial Action Task Force*, FATF)

LCB-FT : Lutte contre le blanchiment de capitaux et le financement du terrorisme

MiCA : Règlement (UE) 2023/1114 sur les marchés de crypto-actifs (*Markets in Crypto-Assets*)

OAT : Outil d'analyse transactionnelle

PSAN : Prestataire de services sur actifs numériques (régime français antérieur au 1er juillet 2026)

PSCA : Prestataire de services sur crypto-actifs (*crypto-asset service provider*, CASP)

TFR : Règlement (UE) 2023/1113 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs

TRACFIN : Traitement du renseignement et action contre les circuits financiers clandestins

INTRODUCTION

Le 15 février 2023, la chambre criminelle de la Cour de cassation tranche une question inédite. La présomption d'origine illicite des biens, posée par l'article 324-1-1 du Code pénal, peut-elle s'appliquer à des bitcoins inscrits sur un compte ouvert auprès d'une plateforme d'échange ? La Cour répond par l'affirmative[1]. Elle le fait sans mobiliser le moindre texte propre aux crypto-actifs : elle étend une catégorie pénale classique à un objet qui n'existait pas lorsque cette catégorie fut conçue. Deux ans plus tard, le législateur consacre cette extension. La loi du 13 juin 2025 visant à sortir la France du piège du narcotrafic complète l'article 324-1-1 d'un alinéa appliquant la présomption à toute opération effectuée « au moyen d'un crypto-actif comportant une fonction d'anonymisation intégrée ou au moyen de tout type de compte ou de technique permettant l'anonymisation ou l'opacification des opérations en crypto-actifs »[2].

Cette méthode n'est pas sans conséquence. Étendre une catégorie existante suppose de la faire coïncider avec un objet qu'elle n'avait pas prévu, opération qui laisse subsister une part d'incertitude sur ce qu'elle exige exactement. Ce qui vaut pour la qualification pénale vaut également pour les obligations de vigilance : les établissements bancaires reçoivent aujourd'hui des flux issus de cet écosystème et doivent leur appliquer des règles conçues pour d'autres circuits. Pour comprendre cette situation, il faut d'abord rappeler ce que sont les crypto-actifs et ce qu'est devenu leur écosystème.

À la fin des années 2000, dans un climat de défiance envers le système financier que la crise bancaire vient d'aggraver, une idée se répand : permettre à deux personnes d'échanger de la valeur sans passer par une banque. Le mécanisme est décrit en 2008 dans un article publié sous le pseudonyme de Satoshi Nakamoto, qui combine des techniques cryptographiques déjà connues plutôt qu'il n'en invente[3]. Il repose sur la blockchain, que le droit français désigne depuis 2017 comme un mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification[4]. La

---

[1]Cass. crim., 15 février 2023, n° 22-81.326, inédit.

[2]Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, JORF du 14 juin 2025.

[3]NAKAMOTO (S.), *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, article publié en ligne sous pseudonyme.

[4]Vocabulaire de l'informatique, JO du 23 mai 2017, v° Chaîne de blocs.

confiance ne repose plus sur une institution mais sur la transparence de ce registre. La première application, Bitcoin, entre en fonctionnement en janvier 2009, et l'ambition d'échanger sans intermédiaire caractérise l'ensemble de l'écosystème qui s'est constitué à sa suite.

L'histoire a pourtant pris le contre-pied de ce projet. L'écosystème s'est considérablement développé : des milliers de crypto-actifs ont suivi, des usages financiers complexes sont apparus, et les investisseurs institutionnels y sont entrés. Mais ce développement s'est fait par la réintroduction de ce qu'il s'agissait de supprimer : les intermédiaires. L'usage direct d'un registre distribué suppose de gérer soi-même ses clés cryptographiques, opération que la plupart des utilisateurs ne maîtrisent pas et dont l'échec entraîne la perte définitive des fonds. Le marché a donc reconstitué des acteurs assurant la conservation, l'échange et la conversion pour le compte de leurs clients, et la doctrine relève que l'écosystème, né d'un postulat de désintermédiation, a évolué vers le recours à de nouveaux intermédiaires[5]. Le règlement sur les marchés de crypto-actifs en prend acte, qui définit non une technologie mais une liste de services rendus à titre professionnel[6].

Un second constat doit être posé, car il conditionne la compréhension du risque. Les crypto-actifs traînent une réputation d'instrument criminel par excellence, nourrie d'affaires retentissantes et de caractéristiques techniques mal comprises. Cette représentation appelle une double nuance.

Quantitativement d'abord. Selon les données du principal fournisseur d'analyse de chaîne, le blanchiment on-chain aurait porté sur environ quatre-vingt-deux milliards de dollars en 2025, montant considérable en valeur absolue mais représentant une fraction résiduelle du volume total des transactions attribuées[7]. Aucune mesure équivalente n'existe pour la monnaie ayant cours légal. La Cour des comptes retient que le blanchiment représenterait trois pour cent du produit intérieur brut mondial et un virgule trois pour cent

[5]PAILLER (P.), « Blanchiment et crypto-actifs : le cadre réglementaire national et européen », *RD bancaire et fin.* 2025, dossier 41.

[6]Règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs, art. 3, § 1, 16), JOUE L 150 du 9 juin 2023, p. 40.

[7]Chainalysis, *Crypto Crime Report* 2026. Ce chiffre, propre au blanchiment on-chain, est distinct du montant total reçu par des adresses illicites la même année (environ cent cinquante-quatre milliards de dollars), dont la hausse est principalement imputable au contournement de sanctions financières, catégorie distincte du blanchiment. Ces données émanent d'un opérateur privé et sont mobilisées comme ordre de grandeur.

de celui de l'Union[8]. Les deux grandeurs ne sont pas comparables. La première est mesurée sur un registre public. La seconde est estimée à partir d'hypothèses macroéconomiques, et les évaluations disponibles varient de un à sept. L'objet réputé le plus opaque est ainsi le seul dont on dispose d'une mesure.

Qualitativement ensuite. Sur les principales blockchains publiques, il n'y a pas d'anonymat mais un pseudonymat : toutes les transactions y sont publiquement consultables et conservées durablement, seule l'identité derrière chaque adresse restant à établir. La doctrine souligne d'ailleurs le caractère contre-intuitif de la situation, les crypto-actifs étant particulièrement traçables, contrairement aux espèces, ce qui a permis le développement d'une industrie spécialisée dans l'analyse transactionnelle des chaînes de blocs[9]. L'arrêt du 15 février 2023 en fournit l'illustration judiciaire : c'est en suivant les transferts inscrits sur la chaîne jusqu'à un compte ouvert auprès d'une plateforme que les enquêteurs ont pu localiser les actifs.

Ces deux constats, la réintermédiation et la traçabilité, orientent la compréhension du risque, à condition de distinguer deux questions : celle de savoir où le risque se situe, et celle de savoir où la prévention peut agir.

Le risque se situe partout. Des fonds d'origine frauduleuse fractionnés entre plusieurs adresses avant d'être regroupés, une valeur transférée d'une chaîne à une autre pour rompre le lien avec son point d'entrée, des actifs déposés sur une adresse contrôlée par un tiers puis restitués sous une autre forme : ces opérations se déroulent intégralement sur la chaîne, sans qu'aucune conversion n'intervienne. Elles n'en dissimulent pas moins l'origine de la valeur, et constituent à ce titre des faits de blanchiment au sens des textes. L'usage illicite de crypto-actifs n'attend pas leur passage en monnaie ayant cours légal pour exister.

La prévention, en revanche, se heurte à une difficulté qui lui est propre. La répression a ses propres moyens : elle recherche un auteur, et l'arrêt précité montre qu'elle sait mobiliser à cette fin la traçabilité du registre. La prévention procède autrement. Elle ne connaît qu'un destinataire possible, l'assujetti, c'est-à-dire une personne à qui la loi impose par avance de

---

[8]Cour des comptes, *L'évolution du dispositif français de lutte contre le blanchiment de capitaux — Exercices 2012-2022*, février 2023, p. 4, reprenant Cour des comptes européenne, rapport spécial n° 13/2021. L'Office des Nations unies contre la drogue et le crime retient une fourchette de deux à cinq pour cent, estimation ancienne et discutée.

[9]SABBAN (D.), « Réglementation LCB-FT et crypto-actifs : des enjeux éminents, des défis persistants », *RD bancaire et fin.* 2025, dossier 43, n° 5.

connaître son client, de surveiller ses opérations et de déclarer ses soupçons. Or, sur la chaîne, il n'existe ni assujetti ni identité, seulement des adresses et des montants. Le dispositif préventif n'y trouve pas de destinataire, non parce que le risque y serait absent, mais parce qu'aucune obligation n'y a de sujet. Ses points d'accroche sont ceux où un acteur identifiable intervient : l'ouverture d'un compte auprès d'une plateforme, la conversion des avoirs en monnaie ayant cours légal, l'entrée des fonds dans le circuit bancaire.

Faute de pouvoir atteindre la circulation elle-même, le législateur européen a porté son effort sur les acteurs qui l'encadrent. Entre 2018 et 2024, l'Union a construit une architecture reposant sur trois instruments. Le règlement MiCA harmonise d'abord le statut des prestataires de services sur crypto-actifs et les soumet à un régime d'agrément[10]. Le règlement dit TFR étend ensuite à ces acteurs l'obligation de faire circuler les informations identifiant l'émetteur et le bénéficiaire de chaque transfert[11]. Le paquet anti-blanchiment de 2024 refond enfin l'ensemble des obligations applicables dans l'Union et institue une autorité européenne de supervision[12].

Les établissements bancaires ne figurent pas parmi les destinataires principaux de ces textes. Ils n'exercent pas de services sur crypto-actifs et ne relèvent pas du régime d'agrément que MiCA institue[13]. Ils n'en sont pas moins exposés à ces flux, par deux voies. La première tient à leurs clients, particuliers ou entreprises, qui convertissent leurs crypto-actifs en monnaie ayant cours légal et virent les fonds sur leur compte. La seconde tient aux prestataires eux-mêmes, qui ont besoin de comptes bancaires pour exercer leur activité, recevoir les dépôts de leurs clients et régler leurs fournisseurs.

Le régime applicable à l'établissement ne fait pas difficulté dans son principe. Les obligations de vigilance, de surveillance et de déclaration de soupçon, définies au niveau européen puis transposées aux articles L. 561-1 et suivants du Code monétaire et financier, valent pour tous les flux qu'il traite, quelle qu'en soit l'origine. La difficulté tient à leur mise en œuvre. Ce que la banque perçoit d'une opération d'origine crypto tient en un virement libellé en euros ; tout ce qui précède lui est invisible. Appliquer une obligation de vigilance

[10]Règlement (UE) 2023/1114, préc.
[11]Règlement (UE) 2023/1113 du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, JOUE L 150 du 9 juin 2023, p. 1.
[12]Règlement (UE) 2024/1624, directive (UE) 2024/1640 et règlement (UE) 2024/1620 du 31 mai 2024, JOUE du 19 juin 2024.
[13]Règlement (UE) 2023/1114, art. 60.

à un tel flux suppose donc de reconstituer une information qu'elle n'a pas constatée elle-même, et qui dépend entièrement de ce qui s'est passé en amont.

C'est cette situation que le présent mémoire se propose d'examiner, et elle appelle une observation qui en constitue le fil directeur. Le dispositif préventif européen repose sur une technique unique : la régulation des intermédiaires. Cette technique consiste à désigner, en chaque point de passage des flux, un professionnel à qui la loi confie une fonction de surveillance. Elle fonctionne aussi longtemps que la chaîne de ces professionnels demeure continue. Lorsqu'elle se rompt, le risque ne disparaît pas : il se présente au dernier maillon subsistant, c'est-à-dire à l'établissement bancaire, qui se trouve alors seul en position de contrôle, sans que la technique employée lui indique ce qui est attendu de lui.

Quatre notions doivent, avant d'aller plus loin, être précisément définies.

Le crypto-actif, d'abord, que le règlement MiCA définit comme une représentation numérique d'une valeur ou d'un droit pouvant être transférée et stockée de manière électronique au moyen de la technologie des registres distribués ou d'une technologie similaire[14], définition convergente avec celle que l'article L. 54-10-1 du Code monétaire et financier, issu de la loi du 22 mai 2019, retenait sous le vocable d'actifs numériques[15].

La blockchain, ensuite, entendue au sens du vocabulaire officiel rappelé plus haut. Le présent mémoire porte sur les blockchains publiques, seules concernées par le double phénomène de transparence du registre et de pseudonymat des utilisateurs.

La lutte contre le blanchiment de capitaux et le financement du terrorisme, en troisième lieu. Le blanchiment, défini à l'article 324-1 du Code pénal, dissimule l'origine criminelle de fonds pour les réinjecter dans l'économie légale, selon les trois phases du placement, de l'empilement et de l'intégration ; le financement du terrorisme, défini à l'article 421-2-2 du même code, s'en distingue en ce que les fonds peuvent être d'origine licite, leur destination caractérisant l'infraction. À cette dimension répressive répond un dispositif préventif reposant sur le triptyque connaissance du client, surveillance des opérations, déclaration de soupçon. Le présent mémoire porte sur ce second volet, la définition pénale n'étant rappelée que pour identifier ce que la prévention a pour objet d'empêcher.

---

[14] *Ibid.*, art. 3, § 1, 5).

[15] C. mon. fin., art. L. 54-10-1, dans sa rédaction issue de la loi n° 2019-486 du 22 mai 2019.

L'effectivité, enfin, entendue comme l'aptitude d'une règle de droit à produire les effets voulus par son auteur dans la réalité sociale[16]. Ce terme est préféré à celui d'efficacité, qui mesurerait l'atteinte des objectifs poursuivis, ou d'adéquation, qui apprécierait la pertinence des moyens retenus. L'effectivité permet en effet de distinguer le droit proclamé du droit opérant, distinction qui traverse l'ensemble du présent propos : il ne s'agit pas de vérifier si les textes existent, ce dont nul ne doute, mais d'observer ce qu'ils produisent lorsqu'il faut les mettre en œuvre.

Le champ de l'analyse appelle quelques précisions. Matériellement, le mémoire porte sur la prévention du blanchiment appliquée aux flux d'origine crypto entrant dans le système bancaire, à l'exclusion de la régulation des prestataires pour elle-même, de la fiscalité des crypto-actifs, de la protection des investisseurs et de la régulation prudentielle. Les textes européens ne sont ainsi étudiés que dans la mesure où ils permettent d'apprécier la capacité des établissements bancaires à mettre en œuvre leurs obligations. Il en résulte une délimitation qu'il convient d'assumer : les usages illicites qui se déroulent et s'achèvent au sein de l'écosystème crypto, sans jamais rejoindre l'économie ordinaire, échappent au présent propos. Ils n'en constituent pas moins des faits répréhensibles, et relèvent d'autres instruments que ceux ici examinés.

Géographiquement, l'analyse est européenne, le droit français étant mobilisé comme transposition et application du droit de l'Union. L'étude ne procède à aucune comparaison de systèmes juridiques : les situations relevant de droits étrangers ne sont mentionnées qu'à titre d'illustration factuelle. Quant à la perspective, le mémoire adopte le point de vue de l'établissement bancaire européen, assujetti aux obligations de vigilance mais dépourvu du statut de prestataire de services sur crypto-actifs. Ce choix tient à la situation singulière de cet acteur, exposé à des flux que les textes propres aux crypto-actifs ne le désignent pas pour traiter, alors que la doctrine s'est surtout attachée à la position des prestataires et à celle des autorités de supervision.

Temporellement, l'analyse porte sur l'état du droit postérieur à MiCA et au paquet anti-blanchiment, dans un moment charnière dont il faut mesurer l'importance. Le régime transitoire des prestataires français s'est achevé le 30 juin 2026[17] ; le règlement anti-

[16]LEROY (Y.), « La notion d'effectivité du droit », *Droit et société*, 2011/3, n° 79, p. 715-732.

[17]Ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs, JORF du 17 octobre 2024, et rectificatif au JORF du 9 novembre 2024. Le rapport au Président de la République précise que les

blanchiment ne sera applicable que le 10 juillet 2027 ; la supervision directe de l'autorité européenne ne débutera que le 1er janvier 2028[18]. Une part substantielle du dispositif décrit dans les développements qui suivent n'est donc pas encore en vigueur, et sera signalée comme telle chaque fois que nécessaire. Décrire au présent un texte qui ne produit pas encore d'effets constituerait une erreur de méthode que le présent travail s'attache à éviter.

La question centrale du mémoire peut alors être formulée. **Dans quelle mesure la régulation par les intermédiaires, retenue pour appréhender les crypto-actifs, permet-elle encore à l'établissement bancaire placé en bout de chaîne d'exercer sa vigilance ?**

La thèse défendue peut être énoncée en une proposition. La technique qui fait tenir le dispositif en amont est celle qui l'affaiblit en aval. Là où la chaîne d'intermédiaires régulés est complète, la banque exerce sa vigilance sur une information qu'elle n'a pas produite. Là où cette chaîne se rompt, elle devient le seul point de contrôle, alors que le référentiel au regard duquel sa diligence sera appréciée ne s'est pas encore formé pour ces flux. Il en résulte une incitation au retrait, dont l'effet est de rompre à son tour la chaîne dont dépendait le dispositif.

L'intérêt du sujet est double. Académique d'abord : la doctrine consacrée à la régulation des crypto-actifs est abondante, mais elle adopte le plus souvent la perspective des prestataires ou celle des autorités de supervision ; la situation de l'établissement bancaire, exposé sans être visé, demeure moins étudiée. Le sujet croise le droit bancaire, le droit financier, le droit pénal des affaires et le droit de l'Union. Pratique ensuite : les établissements traitent des flux d'origine crypto sous un régime applicable mais dont la mise en œuvre soulève des questions non tranchées, et l'analyse de ces questions présente une utilité immédiate pour les praticiens de la conformité.

La méthode combine trois approches. L'analyse de droit positif d'abord, portant sur les règlements MiCA, TFR et anti-blanchiment, la directive de 2024 et le règlement instituant l'autorité européenne, sur les articles L. 561-1 et suivants du Code monétaire et financier, sur les articles 324-1, 324-1-1 et 421-2-2 du Code pénal et la loi du 13 juin 2025, ainsi que sur le droit souple structurant que constituent les orientations de l'Autorité bancaire

---

dispositions mettant définitivement un terme au régime national entrent en application à compter du 1er juillet 2026.

[18]Règlement (UE) 2024/1620, préc. La première procédure de sélection des entités soumises à la supervision directe doit être engagée au plus tard le 1er juillet 2027.

européenne et les lignes directrices des autorités françaises. L'analyse jurisprudentielle ensuite, portant sur la jurisprudence de la Cour de cassation, la pratique décisionnelle de la commission des sanctions et la jurisprudence de la Cour de justice. L'analyse doctrinale et institutionnelle enfin, mobilisant la doctrine française, les rapports du Groupe d'action financière, les analyses de risques publiées par les autorités et les publications des sociétés d'analyse de chaîne, ces dernières étant traitées comme des données factuelles avec la prudence qu'impose leur statut de sources privées.

Trois limites méthodologiques doivent être signalées. Plusieurs textes récents ne produiront leurs effets que dans les prochaines années, ce qui donne à certaines observations une dimension prospective. Les pratiques des établissements ne font l'objet d'aucune publication systématique, de sorte que leur description repose sur les constats des autorités et sur les décisions rendues, non sur une observation directe. Enfin, la dimension opérationnelle du sujet, nécessaire à sa compréhension, n'est abordée qu'en tant qu'elle soulève des questions juridiques.

Le mémoire s'organise en deux chapitres. Le premier examine la technique par laquelle l'Union a construit son dispositif : il en expose les fondements et les instruments, avant d'identifier les situations qu'elle ne saisit pas, tenant à son périmètre comme à son effectivité (Chapitre 1). Le second examine la position dans laquelle cette technique place l'établissement bancaire : il décrit la vigilance que celui-ci met en œuvre et l'information sur laquelle elle repose, avant d'analyser l'indétermination du référentiel au regard duquel elle sera appréciée et les conséquences qui en découlent (Chapitre 2).

CHAPITRE 1 — LA RÉGULATION PAR LES INTERMÉDIAIRES, TECHNIQUE FONDATRICE DU DISPOSITIF EUROPÉEN

Confrontée à l'essor des crypto-actifs, l'Union européenne a construit entre 2018 et 2024 un dispositif reposant sur une décision de méthode : encadrer les personnes qui exploitent la technologie plutôt que la technologie elle-même. Ce choix n'est ni arbitraire ni improvisé ; il prolonge la technique de prévention appliquée au système financier depuis 1991, en l'étendant à une catégorie d'acteurs nouvellement apparue. Encore faut-il en établir les fondements avant d'en mesurer la portée, car une technique fondée sur l'existence d'intermédiaires ne peut rien là où il n'y en a pas. La question se pose ainsi de savoir si ce dispositif appréhende l'ensemble des risques que présentent les crypto-actifs, ou s'il laisse subsister des situations que sa méthode même le rend impuissant à saisir. Le présent chapitre expose d'abord les raisons et les instruments de ce choix (Section 1), avant d'identifier les angles morts qu'il comporte (Section 2).

Section 1 — Le choix de l'intermédiation comme technique de prévention

L'établissement bancaire traditionnel n'est pas prestataire de services sur crypto-actifs. Son exposition naît au point où les crypto-actifs redeviennent de la monnaie ayant cours légal, c'est-à-dire au moment où un virement crédite un compte ouvert dans ses livres. Ce qu'il perçoit alors doit être décrit avec exactitude. Le plus souvent, la contrepartie est identifiable : le virement porte le nom du prestataire émetteur, que le règlement MiCA oblige à déposer les fonds de ses clients auprès d'un établissement de crédit[19]. Ce que la banque ne perçoit pas, c'est l'amont : la manière dont les crypto-actifs convertis ont été acquis, les adresses par lesquelles ils ont transité, l'identité de celui qui les a déposés. Elle hérite ainsi du résultat d'une diligence accomplie par un tiers, sans disposer de la matière qui a permis de la conduire. Certaines configurations effacent en outre la contrepartie elle-même. Les fonds de la clientèle étant cantonnés sur un compte dédié, le client sous-jacent n'apparaît pas ; le recours à un identifiant

[19]Règlement (UE) 2023/1114, art. 70, § 3, relatif à la garde des crypto-actifs et des fonds des clients ; O'RORKE (W.) et NIN (A.), « Prestataires de services sur crypto-actifs », *JurisClasseur Droit bancaire et financier*, fasc. 2505, § 133 et 136.

virtuel redirige le paiement vers un compte différent de celui qu'il désigne[20]. Ce constat commande la manière dont il faut aborder le cadre européen : ce que la banque peut savoir de l'opération dépend entièrement de ce qui s'est passé en amont, et donc de la présence, sur la chaîne de transmission, d'un acteur régulé qui aura lui-même identifié son client. Le choix de méthode opéré par le législateur européen n'est donc pas, pour elle, une question de doctrine réglementaire : il détermine la qualité de l'information qui lui parviendra. Encore faut-il que ce choix soit praticable et qu'il ait été traduit en instruments effectivement applicables. Il convient d'exposer d'abord les fondements qui rendent une régulation par les acteurs à la fois possible et pertinente (§1), avant de présenter les instruments par lesquels ce choix s'est concrétisé et l'état de leur applicabilité (§2).

§1 — Les fondements du choix régulatoire

Deux ordres de considérations expliquent la méthode retenue. Les premières tiennent à ce qu'est devenu l'écosystème crypto, dont deux caractéristiques rendent une telle régulation possible (A). Les secondes tiennent aux méthodes que la lutte contre le blanchiment applique de longue date et qu'elle a progressivement étendues à ce secteur (B).

A. Un écosystème réintermédiarisé et traçable

L'écosystème présente deux propriétés dont le législateur a pu tirer parti : il s'est doté d'intermédiaires professionnels identifiables, et ses registres publics conservent la trace de chaque opération.

1. La reconstitution d'intermédiaires identifiables

L'écosystème des crypto-actifs a été conçu pour fonctionner sans intermédiaire, mais il en a suscité de nouveaux. Cette évolution est la première condition de la méthode retenue par le législateur européen.

Elle s'explique par des contraintes pratiques. L'usage direct d'un registre distribué suppose de gérer soi-même ses clés cryptographiques, opération que la plupart des

[20]Règlement (UE) 2024/1624, art. 22, § 3, non encore applicable ; MEDJAOUI (K.), « Points clés de la réforme du nouveau cadre européen de la lutte contre le blanchiment d'argent et le financement du terrorisme (paquet AML6) », *RD bancaire et fin.* 2025, n° 1, prat. 2. Sur le mécanisme des comptes de transit, V. infra, chapitre 2.

utilisateurs ne maîtrisent pas et dont l'échec entraîne la perte définitive des fonds. Le marché a donc reconstitué des acteurs assurant la conservation, l'échange et la conversion pour le compte de leurs clients. Les enquêtes disponibles confirment cette concentration : deux tiers des détenteurs français déclarent recourir exclusivement à un intermédiaire régulé, l'autodétention pure ne concernant qu'un peu moins d'un quart d'entre eux[21].

Le droit positif enregistre ce mouvement. Le règlement sur les marchés de crypto-actifs ne définit pas une technologie mais une liste de services — conservation et administration pour le compte de tiers, exploitation d'une plateforme de négociation, échange contre des fonds ou contre d'autres crypto-actifs, exécution d'ordres, entre autres. Une telle énumération n'aurait aucun objet si ces fonctions n'étaient pas exercées à titre professionnel par des entités identifiables. Le raisonnement du législateur se lit ainsi en creux dans la structure du texte : ce n'est pas parce qu'il aurait renoncé à saisir la technologie qu'il a régulé les acteurs, c'est parce que la technologie s'était déjà donné des acteurs à saisir.

Cette observation est déterminante pour l'établissement bancaire. Elle signifie que la contrepartie qui se trouve en amont d'un virement de conversion n'est, dans la généralité des cas, ni un anonyme ni un particulier isolé, mais une entreprise soumise à un statut. La vigilance de la banque peut dès lors porter sur une personne identifiée, dont la qualité est vérifiable, et non sur un flux dont l'origine se perdrait dans le registre. Toute la question, examinée à la section suivante, sera de savoir ce qu'il advient dans les hypothèses où cette contrepartie n'existe pas.

2. La traçabilité des blockchains publiques

La seconde caractéristique tient à ce que ces registres ne sont pas opaques. Cette propriété est souvent mal comprise, et sa portée exacte conditionne pourtant l'utilité du cadre réglementaire.

Chaque transaction inscrite sur une blockchain publique est datée, conservée durablement et consultable par tous. Les utilisateurs n'y figurent pas sous leur identité civile mais sous des adresses. Il s'agit donc de pseudonymat et non d'anonymat, distinction que la doctrine souligne constamment et qui commande la suite du raisonnement : une donnée

[21] ADAN et Ipsos, baromètre janvier 2026 : 67 % de recours exclusif à un tiers régulé, en hausse de neuf points en un an, contre 23 % d'autodétention pure et 10 % en mode mixte. Enquête déclarative auprès de 2 000 répondants français. L'ADAN étant l'association professionnelle du secteur, la donnée est mobilisée sous cette réserve et mesure des déclarations d'usage, non des flux.

pseudonyme reste rattachable à une personne pour qui dispose des éléments permettant l'attribution.

La jurisprudence en fournit une illustration précise. Dans l'affaire ayant donné lieu à l'arrêt du 15 février 2023, les investigations avaient été ouvertes à la suite de l'interception de communications chiffrées ; les enquêteurs ont pu suivre sur la chaîne des transferts de bitcoins jusqu'à un compte ouvert auprès d'une plateforme d'échange, et la chambre criminelle a rejeté le pourvoi formé contre la saisie des actifs ainsi localisés.

Cette décision démontre deux choses à la fois, et la seconde importe davantage que la première. Elle établit d'abord que le suivi des flux sur la chaîne est techniquement opérant et judiciairement exploitable. Elle montre surtout que ce suivi n'a produit un résultat qu'au moment où il a rencontré un intermédiaire régulé, seul en mesure de rattacher une adresse à un titulaire identifié. La transparence du registre ne vaut donc pas par elle-même : elle ne devient utile qu'au point de contact avec un acteur soumis à des obligations d'identification.

Il en résulte une conséquence sur laquelle repose l'ensemble du dispositif. Une régulation de l'infrastructure serait dépourvue d'objet quant à la traçabilité, puisque celle-ci existe déjà. L'enjeu réglementaire ne porte pas sur la production de l'information, mais sur les conditions de son attribution à une personne. Cela conduit à examiner la méthode par laquelle la lutte contre le blanchiment organise précisément cette attribution.

B. Une méthode éprouvée, étendue par étapes

Cette méthode, appliquée au système financier depuis 1991, repose sur une délégation de surveillance dont il faut exposer le principe avant d'en retracer l'extension au secteur des crypto-actifs.

1. La fonction de gardien du système financier

La lutte contre le blanchiment ne repose pas sur une surveillance directe des transactions par les autorités publiques, mais sur une délégation de cette fonction aux professionnels qui les traitent. Ce mécanisme est ancien et il n'a pas varié.

Sa logique est simple. Les autorités ne disposent ni des moyens ni de l'accès nécessaires pour observer l'ensemble des flux financiers. La réglementation mobilise donc ceux qui se trouvent au point de passage de ces flux, en leur imposant d'identifier leurs clients, de surveiller leurs opérations et de déclarer leurs soupçons. L'assujetti n'est pas un auxiliaire

occasionnel de l'autorité : il est le destinataire exclusif d'une obligation légale dont l'inexécution est sanctionnée pour elle-même.

Le droit de l'Union porte la trace de cette méthode depuis la directive du 10 juin 1991, et sa constance est remarquable. Six générations de textes se sont succédé, jusqu'au paquet du 31 mai 2024, sans que le principe de la délégation soit jamais remis en cause. Ce qui a changé, à chaque étape, c'est le périmètre des professionnels appelés à l'exercer : d'abord les établissements de crédit, puis les autres entreprises du secteur financier, puis des professions non financières jugées vulnérables, puis les prestataires de services sur crypto-actifs.

Cette permanence éclaire la position de l'établissement bancaire, et elle mérite d'être soulignée car elle est source d'un malentendu fréquent. L'établissement est le destinataire historique de la délégation ; l'extension du dispositif aux prestataires de services sur crypto-actifs ne l'en décharge donc pas. Elle ajoute un assujetti en amont, sans retrancher les obligations de celui qui se trouve en aval. La vigilance du prestataire ne se substitue pas à celle de la banque : elle s'y superpose. Toute la difficulté examinée au second chapitre tient à l'articulation de ces deux vigilances, et à la tentation, pour la seconde, de se reposer sur la première.

2. L'extension aux crypto-actifs de 2018 à 2024

L'extension du dispositif aux crypto-actifs s'est opérée en trois temps, dont la reconstitution éclaire les choix ultérieurs et, singulièrement, la position dans laquelle se trouve aujourd'hui la banque.

La première étape est internationale. La révision de la recommandation 15 du Groupe d'action financière et l'adoption de sa note interprétative tranchent la question de la méthode en soumettant les prestataires de services sur actifs virtuels aux obligations applicables aux institutions financières[22]. Le choix d'encadrer les acteurs plutôt que la technologie est donc arrêté à ce niveau avant d'être transposé, ce qui explique qu'il se retrouve, à l'identique, dans l'ensemble des ordres juridiques qui ont suivi.

La deuxième étape est européenne. La directive du 30 mai 2018 introduit dans le champ des entités assujetties deux catégories seulement : les prestataires de services d'échange entre monnaies virtuelles et monnaies légales, et les prestataires de services de portefeuille de

[22]GAFI, recommandation 15 et sa note interprétative. La recommandation a été amendée en 2018 et sa note interprétative adoptée en 2019.

conservation[23]. Ce périmètre est étroit, et il a été critiqué comme tel. Il est pourtant révélateur du raisonnement suivi : le législateur européen a saisi d'emblée les points de contact entre l'écosystème crypto et le système financier ordinaire, c'est-à-dire précisément les lieux où les valeurs changent de nature.

Cette observation mérite d'être soulignée, car elle conditionne l'angle du présent mémoire. Si le premier périmètre européen visait la conversion, c'est que le point de conversion était identifié comme le point de risque. Or ce point est aussi celui où se situe l'établissement bancaire, à l'autre extrémité de l'opération. L'exposition de la banque n'est donc pas un effet secondaire du dispositif : elle procède de la logique même qui l'a fondé.

La troisième étape est nationale. La loi du 22 mai 2019 dote la France d'un régime propre de prestataire de services sur actifs numériques, articulant un enregistrement obligatoire pour certains services et un agrément facultatif. Ce régime a été étendu l'année suivante, par une ordonnance du 9 décembre 2020, aux services d'échange de crypto-actifs contre d'autres crypto-actifs ainsi qu'à d'autres activités jusque-là hors du champ[24]. Il a fonctionné jusqu'au 30 juin 2026, date à laquelle il a cédé la place au régime européen.

Cette chronologie appelle une conséquence terminologique qui sera observée dans l'ensemble du mémoire. La qualification de prestataire de services sur actifs numériques désigne un régime clos ; celle de prestataire de services sur crypto-actifs désigne le régime en vigueur. Les faits et les décisions antérieurs au 1er juillet 2026 relèvent du premier, et ne peuvent être appréciés au regard du second.

§2 — Les instruments du cadre actuel

Trois textes adoptés entre 2023 et 2024 concrétisent ce choix. Ils n'ont toutefois ni le même objet ni le même degré d'applicabilité, et ils n'atteignent pas l'établissement bancaire de la même manière. Les deux premiers organisent l'accès au marché et la traçabilité des transferts (A). Le troisième harmonise les obligations de vigilance et institue une supervision européenne (B).

---

[23]Directive (UE) 2018/843 du 30 mai 2018, JOUE L 156 du 19 juin 2018, p. 43.

[24]Ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques, JORF du 10 décembre 2020.

A. L'accès au marché et la traçabilité des transferts

Le premier de ces instruments transforme une qualité de fait en statut vérifiable ; le second impose que l'information suive l'opération.

1. MiCA et le statut des prestataires

Le règlement sur les marchés de crypto-actifs ne s'adresse pas à l'établissement bancaire lorsque celui-ci n'exerce aucun service sur crypto-actifs. Son intérêt, pour la banque, est indirect mais considérable : il transforme une qualité de fait, invérifiable, en un statut juridique vérifiable.

Le texte subordonne en effet l'exercice des services sur crypto-actifs à un agrément préalable, délivré selon une procédure définie, et couvrant notamment la conservation, l'exploitation d'une plateforme de négociation, l'échange contre des fonds et l'exécution d'ordres. Il impose des exigences prudentielles, organisationnelles et de gouvernance, ainsi que la protection des fonds des clients, et ouvre en contrepartie un passeport permettant l'exercice dans l'ensemble de l'Union. Le règlement est entré en vigueur le 29 juin 2023 ; il est applicable depuis le 30 décembre 2024, à l'exception de ses titres III et IV relatifs aux jetons adossés à des actifs et aux jetons de monnaie électronique, applicables depuis le 30 juin 2024[25].

Le droit français y ajoute un élément déterminant pour la question examinée ici. L'agrément est délivré par l'Autorité des marchés financiers, mais celle-ci ne peut le délivrer si l'Autorité de contrôle prudentiel et de résolution rend un avis défavorable, notamment sur le dispositif de détection, d'évaluation et de gestion des risques de blanchiment et de financement du terrorisme[26].

L'analyse de cette disposition éclaire la portée réelle de l'agrément pour la banque. Celui-ci ne certifie pas seulement la solidité financière du prestataire : il incorpore une appréciation, par le superviseur bancaire lui-même, de son dispositif de lutte contre le blanchiment. Lorsque la banque vérifie que son client prestataire est agréé, elle ne recueille

---

[25]Règlement (UE) 2023/1114, préc. Entrée en vigueur le 29 juin 2023 ; application au 30 décembre 2024, titres III et IV applicables depuis le 30 juin 2024.

[26]C. mon. fin., art. L. 54-10-7, I, al. 3 : l'avis de l'Autorité de contrôle prudentiel et de résolution est un avis conforme lorsqu'il porte sur les mécanismes, politiques et procédures de contrôle interne destinés à détecter, évaluer et gérer les risques de blanchiment de capitaux et de financement du terrorisme ; O'RORKE (W.) et NIN (A.), fasc. préc. ; BONNEAU (Th.), « Le rôle des autorités de régulation », *RD bancaire et fin.* 2025, n° 2, dossier 12, spéc. n° 12.

donc pas une simple information administrative. Elle constate qu'un contrôle a été exercé sur le point précis qui l'intéresse.

Cette vérification ne saurait pour autant dispenser la banque de ses propres diligences, et la portée exacte de ce constat sera examinée plus loin. Elle constitue néanmoins le premier apport concret du cadre européen à la situation de l'établissement bancaire : elle lui fournit un fait vérifiable là où il n'avait qu'une réputation à apprécier.

2. Le règlement TFR et la règle du voyage

Le second règlement complète ce statut par une obligation de traçabilité. Il est, des trois instruments examinés, le seul qui atteigne directement l'établissement bancaire.

Le principe est celui de l'accompagnement : chaque transfert doit être assorti des informations identifiant le donneur d'ordre et le bénéficiaire, transmises avec l'opération elle-même[27]. Le texte européen se montre plus exigeant que le standard international, puisqu'il ne retient aucun seuil pour les transferts de crypto-actifs entre prestataires, et il étend l'obligation aux transferts impliquant un portefeuille auto-hébergé. Le prestataire intermédiaire, défini comme celui qui n'est ni le prestataire de l'initiateur ni celui du bénéficiaire mais qui reçoit et transmet un transfert pour le compte de l'un d'eux, est lui-même soumis à des obligations propres[28]. Les orientations adoptées par l'Autorité bancaire européenne le 4 juillet 2024 précisent les modalités de mise en œuvre de ces exigences[29].

La transposition française confirme la portée de cet instrument pour les établissements de crédit. L'ordonnance du 15 octobre 2024 relative au renforcement des obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme en matière de transfert de crypto-actifs prévoit notamment une vigilance renforcée lorsque le transfert implique une adresse auto-hébergée[30]. Son décret d'application, du 23 décembre 2024, vise expressément parmi ses publics concernés les prestataires de services sur crypto-actifs, les établissements de crédit et les établissements de monnaie électronique, et impose, en cas de relation

---

[27]Règlement (UE) 2023/1113, art. 14 et s.

[28]*Ibid.*, art. 3, 16), et art. 19 et s.

[29]Autorité bancaire européenne, orientations EBA/GL/2024/11 du 4 juillet 2024, applicables depuis le 30 décembre 2024.

[30]Ordonnance n° 2024-937 du 15 octobre 2024 relative au renforcement des obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme en matière de transfert de crypto-actifs, JORF du 17 octobre 2024 ; C. mon. fin., art. L. 561-10-4.

transfrontalière de correspondant impliquant l'exécution de services sur crypto-actifs, de vérifier au moment de nouer la relation d'affaires si l'entité cliente est agréée ou enregistrée[31].

Cette disposition mérite une attention particulière, car elle constitue à ce jour le seul texte réglementaire français qui fasse peser sur la banque une obligation expresse et spécifique à raison de son exposition aux crypto-actifs. Son contenu est cependant limité à deux égards : elle ne joue que dans les relations transfrontalières, et elle se borne à imposer la vérification d'un agrément. Elle établit ainsi un seuil minimal de diligence, sans indiquer ce qui est attendu au-delà, première manifestation d'une indétermination dont le second chapitre montrera l'étendue.

À la traçabilité technique de la chaîne, qui identifie des adresses, s'ajoute donc une traçabilité juridique, qui identifie des personnes. C'est par ce canal, et non par la lecture du registre, que la banque accède à une information exploitable sur une opération qu'elle n'a pas elle-même exécutée. Ce constat est essentiel : l'information dont dispose la banque n'est pas produite par elle, mais transmise par d'autres, et sa qualité dépend donc entièrement de la diligence de ces derniers.

B. L'harmonisation des obligations et la supervision européenne

Le paquet de 2024 uniformise les obligations par le recours au règlement et dote la supervision d'un échelon européen.

1. Le paquet anti-blanchiment de 2024

Le paquet adopté le 31 mai 2024 et publié au Journal officiel de l'Union européenne le 19 juin suivant fait des prestataires de services sur crypto-actifs des entités assujetties à part entière, soumises aux mêmes obligations de vigilance, de conservation et de déclaration que les autres entités financières. Il comporte des dispositions propres aux risques du secteur, au premier rang desquelles des mesures d'atténuation applicables aux transactions effectuées au moyen d'une adresse auto-hébergée et une interdiction de tenir des comptes anonymes de crypto-actifs[32].

Le changement d'instrument est ici plus significatif que le changement de contenu. Jusqu'alors, l'assujettissement procédait de directives, dont la transposition laissait aux États

[31]Décret n° 2024-1205 du 23 décembre 2024, JORF n° 0304 du 24 décembre 2024, texte n° 17.
[32]Règlement (UE) 2024/1624, art. 40 et art. 79, § 1.

membres une marge d'appréciation. Il résulte désormais d'un règlement directement applicable, ce qui met fin aux divergences nationales que le législateur européen avait lui-même identifiées comme un facteur de fragmentation.

Cette harmonisation intéresse directement l'établissement bancaire, pour une raison qui tient à la structure de son exposition. La banque française reçoit des flux provenant de prestataires établis dans d'autres États membres. Le degré de confiance qu'elle peut accorder aux diligences accomplies en amont dépend donc de l'uniformité des obligations qui s'y appliquent. Tant que ces obligations variaient d'un État à l'autre, l'appartenance à l'Union ne garantissait pas un niveau d'exigence homogène ; le recours au règlement corrige ce défaut, du moins en principe. La réserve n'est pas de style : l'uniformité de la règle ne garantit pas l'uniformité de son application, et la section suivante montrera que l'écart entre les deux constitue précisément l'une des faiblesses du dispositif.

2. L'autorité européenne et le calendrier de mise en œuvre

Le paquet institue en outre une autorité européenne de lutte contre le blanchiment, chargée de superviser directement certaines entités et de coordonner les autorités nationales. La supervision, jusqu'alors exclusivement nationale, se dote ainsi d'un échelon européen. L'autorité, dont le siège a été fixé à Francfort-sur-le-Main, est opérationnelle depuis le 1er juillet 2025 et a repris au 1er janvier 2026 les mandats en matière de lutte contre le blanchiment auparavant exercés par l'Autorité bancaire européenne. Les prestataires de services sur crypto-actifs figurent parmi les entités susceptibles de relever de cette supervision directe[33]. La sélection obéit toutefois à deux critères cumulatifs : exercer son activité dans au moins six États membres, et présenter un profil de risque élevé. Une quarantaine d'entités seulement devraient être retenues, tous secteurs confondus[34]. Le critère déterminant est donc l'implantation transfrontalière, non l'exposition aux flux d'origine crypto. Un prestataire actif dans cinq États membres demeure sous supervision nationale, quel que soit son profil, et reste ainsi soumis aux disparités d'application examinées à la section suivante.

[33]MEDJAOUI (K.), art. préc., *RD bancaire et fin.* 2025, n° 1, prat. 2 ; SABBAN (D.), art. préc., dossier 43, n° 18, qui relève que la méthode de supervision reste à définir par l'autorité.
[34]Règlement (UE) 2024/1620, art. 12, § 1 ; LYON LYNCH (O.), « L'AMLA/ALBC et le secteur financier », *RD bancaire et fin.* 2025, n° 5, dossier 27, n° 11 à 17.

Le calendrier commande toutefois la portée de ces développements, et il doit être exposé avec précision car il conditionne la qualification juridique des développements qui suivent. Le règlement instituant l'autorité s'applique depuis le 1er juillet 2025. Le règlement harmonisant les obligations de vigilance ne s'appliquera qu'à compter du 10 juillet 2027, certaines catégories d'entités n'y étant soumises qu'à compter du 10 juillet 2029. La directive du même jour, entrée en vigueur le 9 juillet 2024, doit être transposée au plus tard le 10 juillet 2027. Quant à la supervision directe, elle ne débutera qu'au 1er janvier 2028, la première procédure de sélection devant être engagée au plus tard le 1er juillet 2027 et ne portant que sur un nombre restreint d'entités transfrontalières[35].

Il en découle une conséquence méthodologique majeure. Le règlement harmonisant les obligations de vigilance ne régit pas encore les diligences des établissements assujettis, et il ne peut être décrit qu'au futur. À la date de rédaction du présent mémoire, l'établissement bancaire français demeure soumis aux articles L. 561-1 et suivants du Code monétaire et financier dans leur rédaction issue des directives antérieures, complétés par les textes propres aux transferts de crypto-actifs examinés plus haut.

Une seconde incertitude s'ajoute à la première, et elle est d'une autre nature. Le règlement européen renvoie à des normes techniques de réglementation le soin de préciser une part substantielle des obligations de vigilance, et ces normes ne sont pas adoptées. L'établissement se trouve ainsi placé dans une situation singulière : il lui faut préparer l'application d'un régime dont il connaît la date d'entrée en jeu mais non le contenu précis des exigences qui en découleront. Cette configuration n'est pas propre au secteur des crypto-actifs, mais elle y produit des effets particuliers, car c'est précisément sur ce terrain que les questions opérationnelles demeurent les moins tranchées.

L'architecture ainsi constituée est cohérente : elle identifie des acteurs, leur assigne des obligations éprouvées et se dote des moyens de les contrôler. La cohérence d'un dispositif ne préjuge toutefois pas de son étendue. Il reste à examiner ce qu'il atteint effectivement.

[35]Règlement (UE) 2024/1620, préc. ; règlement (UE) 2024/1624, applicable à compter du 10 juillet 2027 ; directive (UE) 2024/1640, entrée en vigueur le 9 juillet 2024, transposition au 10 juillet 2027.

Section 2 — Les angles morts de l'intermédiation

La technique retenue suppose trois conditions : que les flux transitent par des acteurs juridiquement saisissables, que l'information circule effectivement entre eux, et que le respect de leurs obligations soit contrôlé. Aucune n'est pleinement satisfaite. Il importe de préciser d'emblée la nature de ce constat : il ne s'agit pas de recenser des défauts de rédaction que le législateur aurait pu éviter, mais d'identifier les conséquences nécessaires du choix de méthode exposé plus haut. Une régulation qui saisit des personnes est par construction impuissante là où il n'y a pas de personne à saisir, et une obligation qui repose sur la transmission d'une information ne vaut que ce que vaut la chaîne de ceux qui la transmettent. Les défaillances de la première condition tiennent au périmètre du dispositif (§1) ; celles des deux autres tiennent à son effectivité (§2).

§1 — Les limites inhérentes au périmètre

Deux hypothèses échappent au cadre, et il importe de ne pas les confondre. Dans la première, un service est bien rendu, mais par une personne que le droit de l'Union ne peut atteindre, soit qu'elle n'existe pas juridiquement, soit qu'elle se situe hors de sa portée territoriale (A). Dans la seconde, la valeur circule sans qu'aucun service soit rendu par quiconque (B).

A. Les acteurs hors d'atteinte

Deux situations doivent être distinguées, selon que nul n'exerce le service ou qu'un acteur l'exerce hors de portée du droit de l'Union.

1. Les protocoles décentralisés sans opérateur

Le règlement MiCA exclut de son champ les services fournis de manière totalement décentralisée. Cette exclusion n'est pas un oubli : elle est la conséquence logique de la méthode retenue. Là où nul n'exerce le service, nul ne peut être agréé, ni surveillé, ni sanctionné. Une régulation par les acteurs suppose un acteur ; en son absence, elle n'a pas d'objet.

L'exclusion n'est toutefois ni générale ni automatique, et son appréciation soulève des difficultés considérables. Les autorités nationales ont dû élaborer des critères permettant de

déterminer si un protocole est effectivement décentralisé ou si une personne conserve, en fait, une maîtrise suffisante pour être qualifiée de prestataire. L'autorité de supervision danoise a ainsi publié en juin 2024 des principes d'appréciation de la décentralisation en matière de crypto-actifs[36], démarche qui témoigne d'une double réalité : la nécessité d'un test, et l'absence de test harmonisé au niveau de l'Union.

La question demeure ouverte au niveau européen. Le règlement lui-même prévoyait l'établissement d'un rapport conjoint des autorités européennes de surveillance sur les développements récents en matière de crypto-actifs, publié en janvier 2025[37], et l'exercice doit être renouvelé. La perspective d'une extension du cadre à la finance décentralisée reste ainsi à l'état de travaux préparatoires, ce qui signifie que la lacune subsistera pour toute la durée d'application du dispositif examiné dans le présent mémoire. Les deux autorités relèvent d'ailleurs que le règlement ne couvre ni le prêt, ni l'emprunt, ni les services pleinement décentralisés. Une décision étrangère illustre concrètement cette limite. Un tribunal néerlandais a condamné en 2024 l'un des développeurs d'un protocole de mixage à raison des usages qui en avaient été faits, écartant l'argument tiré de ce qu'il n'exerçait plus aucune influence sur des contrats intelligents fonctionnant de manière autonome ; les juges ont toutefois reconnu que l'arrêt du protocole était devenu virtuellement impossible[38]. Là où nul opérateur ne peut être contraint, la réponse se déplace vers la personne du développeur, sans que le protocole cesse pour autant de fonctionner.

Il faut mesurer ce que cela implique pour l'établissement bancaire. Un flux ayant transité par un protocole décentralisé n'est pas seulement dépourvu des informations que la règle du voyage aurait imposé de transmettre : il est dépourvu de tout assujetti ayant eu, à un moment quelconque, l'obligation de connaître son auteur. Lorsque ce flux se présente à la banque après conversion, celle-ci n'est pas confrontée à une information incomplète, mais à une information inexistante. Elle se trouve alors, non pas en position de vérifier ce qu'un autre a

---

[36]Finanstilsynet, *Principles for the assessment of decentralisation in the markets for crypto-assets*, 25 juin 2024.

[37]Autorité bancaire européenne et Autorité européenne des marchés financiers, rapport conjoint EBA/Rep/2025/01 – ESMA75-453128700-1391, 16 janvier 2025 (RD bancaire et fin. 2025, n° 2, alerte 52) : la valeur bloquée dans les protocoles de finance décentralisée y est évaluée à quatre pour cent de la valeur totale du marché mondial des crypto-actifs.

[38]Rechtbank Oost-Brabant, 14 mai 2024, affaire dite Tornado Cash, condamnation à soixante-quatre mois d'emprisonnement, décision frappée d'appel. Élément de fait rapporté à titre d'illustration, à l'exclusion de toute analyse de droit néerlandais.

constaté, mais en position de constater seule — sans que le dispositif lui ait indiqué comment.

2. Les prestataires établis hors de l'Union

La seconde hypothèse est d'une autre nature : un acteur existe et exerce le service, mais il n'est pas soumis au droit de l'Union.

Le règlement MiCA repose sur une présomption de territorialité : le service est réputé fourni dans l'Union lorsqu'il est proposé à des clients qui y sont établis, ce qui soumet le prestataire à l'obligation d'agrément. Cette présomption connaît toutefois une exception, celle de la sollicitation inversée, qui joue lorsque le service est rendu à l'initiative exclusive du client. L'Autorité européenne des marchés financiers a adopté le 26 février 2025 des orientations relatives à cette exemption, dont le caractère dérogatoire commande une interprétation restrictive[39].

La doctrine relève que cette configuration constitue une limite structurelle du dispositif. Les transactions sur crypto-actifs ont fréquemment une dimension transfrontalière, et un prestataire de pays tiers non agréé au titre du droit de l'Union peut parfaitement intervenir dans la chaîne de transfert ; s'il ne peut solliciter des clients domiciliés dans l'Union, ces derniers peuvent le solliciter volontairement. Les facteurs de risque tiennent alors à la localisation de ce prestataire : établissement dans un pays faisant l'objet de mesures restrictives, dans un pays dont le dispositif de lutte contre le blanchiment est jugé déficient, ou dans un pays ne prévoyant aucun agrément[40].

Les données du Groupe d'action financière permettent de mesurer l'ampleur du phénomène, et elles sont éclairantes. Sur cent trente-huit juridictions évaluées au titre de la recommandation 15 en avril 2025, une seule est pleinement conforme ; quarante, soit vingt-neuf pour cent, sont largement conformes ; vingt-neuf, soit vingt et un pour cent, sont non conformes, le solde n'étant que partiellement conforme. Si quatre-vingt-deux pour cent des juridictions ont défini une approche réglementaire, trente-trois pour cent seulement imposent effectivement un agrément en pratique. L'organisme identifie par ailleurs des lacunes

[39]Autorité européenne des marchés financiers, orientations ESMA35-1872330276-2030 du 26 février 2025, relatives à l'article 61 du règlement (UE) 2023/1114.
[40]PAILLER (P.), art. préc., n° 16.

persistantes en matière d'agrément, d'enregistrement, d'identification des prestataires et de surveillance des plateformes offshore[41].

Le législateur européen a lui-même mesuré la portée de cette limite, ce qui doit être souligné car il s'agit d'une reconnaissance institutionnelle et non d'une critique doctrinale. Le règlement sur les transferts prévoit en effet une clause de réexamen, sur la base d'un rapport de la Commission européenne évaluant les risques que présentent les transferts vers ou depuis des entités non agréées[42]. Le dispositif comporte donc, dès sa conception, l'aveu que son périmètre territorial ne coïncide pas avec celui des flux qu'il prétend saisir. Une affaire française en fournit l'illustration. Une plateforme d'échange enregistrée à Hong Kong, opérant en russe et en anglais, était accessible aux clients français ; l'enquête a établi qu'une part considérable des actifs qui y transitaient était liée à des activités criminelles. Seule une opération judiciaire internationale a permis d'y mettre fin[43]. Le prestataire n'était soumis à aucune obligation de vigilance au titre du droit de l'Union : il n'a pu être atteint que par la voie répressive, et après coup.

B. La circulation hors intermédiaire

Cette hypothèse se distingue des précédentes en ce qu'elle ne suppose aucun acteur, et elle prend sa mesure au regard des instruments effectivement employés.

1. Les portefeuilles auto-hébergés

Les obligations existantes supposent toutes l'intervention d'un prestataire, y compris celles qui visent les portefeuilles auto-hébergés. Cette précision est capitale et elle est fréquemment mal comprise : lorsque le règlement sur les transferts impose des diligences relatives à une adresse auto-hébergée, il ne fait pas peser une obligation sur le détenteur du portefeuille, mais sur le prestataire qui exécute le transfert vers cette adresse ou depuis elle. La règle ne saisit pas le portefeuille : elle saisit l'intermédiaire qui le rencontre.

Il en résulte que les transferts opérés directement entre deux portefeuilles auto-hébergés échappent entièrement au dispositif. Aucun assujetti n'intervient, donc aucune obligation n'a

---

[41]GAFI, *Targeted Update*, juin 2025, données arrêtées au mois d'avril 2025.

[42]Règlement (UE) 2023/1113, clause de réexamen ; PAILLER (P.), art. préc., n° 17.

[43]Parquet du tribunal judiciaire de Paris, communiqué du 18 janvier 2023 ; opération conduite par le commandement de la gendarmerie dans le cyberespace avec le concours d'Europol et des autorités américaines. Élément de fait rapporté à titre d'illustration.

de sujet, donc aucune information n'est collectée. Une valeur peut ainsi changer de mains un nombre indéterminé de fois sans que quiconque ait été en position de recueillir la moindre donnée sur les parties.

Le droit français et le droit européen ont tiré de ce constat une conséquence qui en confirme l'analyse. L'ordonnance du 15 octobre 2024 prévoit une vigilance renforcée lorsque le transfert implique une adresse auto-hébergée, et le règlement anti-blanchiment de 2024 comporte des mesures d'atténuation des risques liés aux transactions effectuées au moyen d'une telle adresse. Ces dispositions ne comblent pas la lacune : elles la contournent, en renforçant les diligences au point de contact avec le système régulé, faute de pouvoir agir sur le segment qui lui échappe. Elles confirment ainsi, par leur technique même, que le dispositif ne peut agir que là où un assujetti se trouve.

2. Les techniques d'opacification et la réponse pénale

La lacune prend toute sa mesure au regard des techniques destinées à rompre la traçabilité. Les services de mixage combinent les fonds de plusieurs utilisateurs afin de masquer l'origine des sommes, les crypto-actifs étant ensuite redistribués par transactions fragmentées de manière à rompre le lien entre l'adresse d'entrée et l'adresse de sortie. S'y ajoutent les crypto-actifs dotés d'une fonction d'anonymisation renforcée, ainsi que les schémas consistant à faire transiter rapidement les actifs entre plusieurs chaînes[44].

Ces procédés ne forment pas une catégorie homogène. La doctrine en distingue plusieurs strates : masquer l'accès au réseau, confier les avoirs à un tiers selon un mécanisme intégré à l'algorithme, chiffrer le registre lui-même, ou en supprimer la mémoire par une preuve à divulgation nulle de connaissance[45]. La distinction n'est pas théorique : elle commande la portée des textes qui visent les crypto-actifs comportant une fonction d'anonymisation intégrée, formule qui ne saisit pas les mêmes réalités techniques selon la strate considérée. Le droit européen n'ignore pas ces techniques, mais il ne peut les atteindre qu'indirectement, par le canal des acteurs. Le règlement MiCA prévoit ainsi que les crypto-actifs dotés de fonctions d'anonymisation ne peuvent être admis à la négociation que si leur traçabilité est

[44]LEGEAIS (D.), « Loi narcotrafic et blanchiment de crypto-actifs », *RD bancaire et fin.* 2025, comm. 85 ; VASQUES (V.) et COTIER (J.-F.), « La LCB-FT au cœur de la sécurité des services sur actifs numériques », *Revue Banque*, janv. 2024.

[45]CLÉMENT (S.) et LELIEUR (J.), « La conformité anti-blanchiment face aux crypto-actifs », *RSC* 2021, n° 1, p. 15 et s., spéc. p. 26-27. L'article est antérieur au règlement MiCA et au paquet de 2024 ; il n'est mobilisé que pour la description des procédés techniques.

assurée[46]. La disposition est significative de la méthode : elle ne prohibe pas l'instrument, elle conditionne son accès à une plateforme régulée. Là encore, la contrainte ne s'exerce qu'au point de contact.

C'est précisément parce que la voie préventive est ainsi bornée que le législateur français a déplacé la contrainte vers l'aval répressif. La loi du 13 juin 2025 étend la présomption de blanchiment de l'article 324-1-1 du Code pénal aux opérations réalisées au moyen d'un crypto-actif comportant une fonction d'anonymisation intégrée ou de toute technique permettant l'anonymisation ou l'opacification des opérations, et modifie dans le même sens l'article 415-1 du Code des douanes[47]. Le mécanisme retenu est un renversement de la charge de la preuve : il incombera à la personne poursuivie de justifier que le recours à une telle technique poursuivait une finalité autre que la dissimulation.

Ce déplacement mérite d'être analysé plutôt que simplement constaté. Il révèle un aveu d'impuissance préventive : faute de pouvoir imposer une obligation à celui qui exploite un mixeur, le législateur sanctionne plus aisément celui qui y recourt. Mais il ne fournit à l'établissement bancaire aucun instrument supplémentaire. La présomption pénale joue devant le juge répressif, une fois les faits établis ; elle ne dit rien de ce que la banque devait détecter au moment où le virement s'est présenté. Les démantèlements successifs de services de mixage, conduits par des autorités européennes entre 2023 et 2025, confirment ce déplacement : ces services ont été atteints par la saisie de leurs serveurs et de leurs noms de domaine, non par une obligation qui aurait pesé sur leurs exploitants[48]. L'écart entre la sévérité de la réponse répressive et le silence de la règle préventive constitue l'une des données de la situation examinée au second chapitre.

§2 — Les limites tenant à l'effectivité

Les développements qui précèdent portaient sur ce que le dispositif ne peut pas atteindre. Il faut à présent examiner ce qu'il atteint sans le maîtriser. L'information censée circuler entre acteurs régulés y parvient imparfaitement (A), et le contrôle du respect des obligations demeure d'une portée limitée (B).

---

[46]Règlement (UE) 2023/1114, art. 76, § 3.

[47]Loi n° 2025-532 du 13 juin 2025, préc. ; C. pén., art. 324-1-1 ; C. douanes, art. 415-1.

[48]Europol, communiqué du 26 novembre 2025, démantèlement du service Cryptomixer en coopération avec les autorités allemandes et suisses ; précédemment, démantèlement du service ChipMixer en mars 2023. Éléments de fait rapportés à titre d'illustration.

A. La circulation imparfaite de l'information

Deux obstacles doivent être distingués, l'un technique, l'autre géographique.

1. Les limites techniques de la transmission

La règle du voyage impose un résultat sans imposer de canal. Plusieurs solutions techniques concurrentes se sont donc développées, sans garantie d'interopérabilité, et le Groupe d'action financière relève que les prestataires régulés pâtissent de ce défaut d'interopérabilité entre les outils de conformité[49].

Les insuffisances relevées sont précises et méritent d'être rapportées, car elles montrent que l'obligation peut être formellement respectée tout en étant matériellement inopérante. Certains outils ne sont conçus que pour identifier les contreparties abonnées au même outil, ce qui restreint leur utilité aux transactions internes à un écosystème donné. D'autres transmettent l'information après l'inscription de la transaction sur la chaîne, alors que le respect des obligations de gel suppose une transmission en temps utile[50]. Une juridiction a rapporté avoir imposé des injonctions réglementaires à un prestataire pour non-conformité tenant aux déficiences de son outil, telles qu'une couverture incomplète des actifs virtuels traités ou une transmission tardive des données[51].

Ce constat appelle une observation qui vaut pour l'ensemble du présent chapitre. L'obligation est respectée dans son principe mais imparfaitement exécutée : l'information transmise peut être partielle, tardive ou incompatible avec le système du destinataire. Or l'établissement bancaire situé en fin de chaîne ne reçoit pas cette information directement ; il en reçoit, le cas échéant, le produit filtré par le prestataire qui la lui transmet. Les défaillances de la chaîne amont ne lui sont donc pas visibles : il ignore, en recevant un virement, si l'information qui l'accompagne est complète ou si elle a été dégradée en cours de route.

---

[49]GAFI, *Targeted Update*, juin 2024.
[50]GAFI, *Targeted Update*, juin 2023.
[51]GAFI, *Targeted Update*, juin 2024.

2. L'inégale application entre juridictions

À cette difficulté s'ajoute celle que le Groupe d'action financière désigne sous le nom de *sunrise issue*, tenant à l'adoption inégale de la règle selon les juridictions[52]. Le phénomène a été relevé dès le premier *Targeted Update*, en 2022 : l'application inégale conduit certains prestataires à interagir avec des contreparties étrangères qui ne sont soumises à aucune exigence équivalente[53]. Tant que la règle n'est pas généralisée, les prestataires conformes supportent seuls la charge de la conformité, sans que leur diligence produise l'effet recherché, puisque la contrepartie ne leur transmet rien.

L'ampleur de la difficulté a été mesurée. En 2024, quinze pour cent des juridictions ayant adopté une législation sur la règle du voyage, soit dix sur soixante-cinq, permettaient encore à leurs prestataires nationaux de transacter avec n'importe quel prestataire étranger, quel que soit son statut d'agrément, sa conformité à la règle ou les mesures d'atténuation prises[54]. L'organisme international en tirait la conclusion que la difficulté ne serait résolue que par une mise en œuvre généralisée de ses standards.

Le phénomène évolue toutefois sans disparaître, et sa transformation est plus instructive que sa persistance. Les données les plus récentes indiquent que quatre-vingt-trois pour cent des juridictions interrogées disposent désormais d'une législation en vigueur, contre soixante-treize pour cent l'année précédente. Mais sur les quatre-vingt-onze juridictions concernées, cinquante-cinq, soit soixante pour cent, n'ont émis aucun constat, aucune directive ni aucune mesure d'exécution en matière de conformité à la règle du voyage[55]. La difficulté s'est donc déplacée : la contrepartie est désormais souvent soumise à une obligation, sans que le respect de celle-ci soit vérifié. Ce déplacement est capital pour le raisonnement suivi ici, car il transforme la nature de l'incertitude. L'établissement qui reçoit un flux ne peut plus se rassurer en constatant que la juridiction d'origine s'est dotée d'une règle : l'existence de la règle ne renseigne plus sur son observation.

---

[52]GAFI, *Targeted Update*, juin 2024, encadré « Sunrise Issue » : les retards et incohérences dans la transposition nationale de la règle du voyage produisent cette difficulté, la conformité supposant que le prestataire de l'initiateur et celui du bénéficiaire y soient l'un et l'autre tenus.

[53]GAFI, *Targeted Update*, juin 2022.

[54]GAFI, *Targeted Update*, juin 2024.

[55]GAFI, *Targeted Update*, juillet 2026.

B. La portée limitée du contrôle

Le constat vaut au niveau international comme au niveau national.

1. Le déficit international de supervision

Les données du Groupe d'action financière font apparaître un décalage constant entre l'adoption des règles et leur mise en œuvre coercitive. En 2025, soixante-treize pour cent des juridictions avaient adopté une législation relative à la règle du voyage, mais cinquante-neuf pour cent ne l'avaient pas mise en application[56]. Le rapport le plus récent confirme la tendance : parmi les juridictions dont la législation est en vigueur, une majorité n'a engagé aucune action de supervision fondée sur son non-respect, l'organisme attribuant partiellement cet écart au caractère récent des textes et à la construction encore inachevée des cadres de supervision[57].

La règle existe donc largement ; son respect est peu vérifié. Cette observation ne relève pas du constat désabusé : elle a une portée juridique directe pour l'établissement bancaire. La confiance qu'il peut accorder à un prestataire étranger repose, en dernière analyse, sur l'hypothèse qu'un superviseur exerce sur lui un contrôle. Lorsque cette hypothèse est démentie par les données publiées par l'organisme qui a conçu le standard lui-même, l'établissement se trouve privé du fondement de sa propre appréciation.

Il faut ajouter que le standard international dont procède le dispositif européen est lui-même en cours de refonte. La recommandation 16, qui porte la règle du voyage, a fait l'objet d'une révision destinée à harmoniser les exigences de données, dont la mise en œuvre s'étalera sur plusieurs années[58]. Au moment où l'Union achève de bâtir son édifice, le socle international sur lequel il repose se déplace.

2. L'absence de contentieux disciplinaire national

Le constat se vérifie au niveau national, dans des termes toutefois différents. Les prestataires français sont soumis à la supervision de l'Autorité de contrôle prudentiel et de résolution depuis 2019, et aucune décision de sa commission des sanctions n'a été publiée à leur encontre.

---

[56]GAFI, *Targeted Update*, juin 2025.
[57]GAFI, *Targeted Update*, juillet 2026 ; GAFI, *Best Practices in Travel Rule Supervision*, 2025.
[58]GAFI, révision de la recommandation 16 adoptée le 18 juin 2025.

Ce constat appelle la plus grande prudence dans son interprétation, et il doit être présenté pour ce qu'il est : un indice, non une démonstration. L'absence de sanction peut tenir à la jeunesse du régime, à des procédures en cours et non encore closes, au traitement de certaines situations par le refus ou le retrait d'enregistrement plutôt que par la voie disciplinaire, ou encore à une conformité satisfaisante du secteur. Aucune de ces hypothèses ne peut être écartée, et l'honnêteté méthodologique commande de ne pas conclure de l'absence de décision à l'absence de contrôle.

L'observation conserve néanmoins une portée, et elle est double. D'une part, elle prive l'établissement bancaire de tout référentiel : le standard de diligence attendu d'un prestataire de services sur crypto-actifs, en droit français, ne s'est jamais exprimé dans une décision. La banque qui doit apprécier le dispositif de son client prestataire ne dispose donc d'aucun point de comparaison. D'autre part, le contraste avec l'activité répressive, plus visible et récemment renforcée par la loi du 13 juin 2025, suggère que la voie préventive n'a pas encore produit ses effets propres dans ce secteur.

Le cadre européen atteint les acteurs qu'il désigne, mais laisse subsister des situations qu'il ne saisit pas et des obligations dont le respect demeure inégalement contrôlé. Ces deux séries de limites ne sont pas des imperfections accidentelles : elles procèdent de la technique retenue, qui ne peut agir que sur des personnes et par leur intermédiaire. Les risques correspondants ne disparaissent pas pour autant. Ils se présentent, en fin de parcours, à l'établissement bancaire qui reçoit les fonds convertis, et qui se trouve être, dans nombre d'hypothèses, le premier assujetti à les rencontrer. Il convient dès lors d'examiner la manière dont il y répond, et le référentiel au regard duquel sa réponse sera jugée.

CHAPITRE 2 — L'ÉTABLISSEMENT BANCAIRE, DÉBITEUR D'UNE VIGILANCE SANS RÉFÉRENTIEL CONSTITUÉ

L'établissement bancaire n'exerce aucun service sur crypto-actifs et ne relève pas du régime d'agrément institué par MiCA. Cette position procède d'un choix et non d'une contrainte, puisque le règlement lui ouvre l'accès à ces services par simple notification. Il n'en reçoit pas moins les flux convertis, par ses clients comme par les prestataires qui ont besoin de comptes pour exercer, et il leur applique les obligations de vigilance du droit commun. Pour ce faire, il a dû concevoir des dispositifs spécifiques, car ce qu'il perçoit d'une opération d'origine crypto se réduit à un virement libellé en euros. Deux questions se posent alors, et elles commandent la structure du présent chapitre. Sur quoi cette vigilance repose-t-elle, dès lors que l'établissement n'a rien constaté par lui-même (Section 1) ? Et au regard de quel référentiel sa conduite sera-t-elle appréciée (Section 2) ?

Section 1 — Une vigilance construite sur une information exogène

Appliquer une obligation de vigilance à un flux d'origine crypto suppose deux opérations successives : identifier les risques que ce flux présente, puis disposer des moyens de les détecter. L'identification suppose la connaissance des schémas et leur traduction en critères opérationnels (§1) ; la détection mobilise des moyens spécifiques (§2). Ces deux opérations ont une caractéristique commune, qui commande l'analyse de la section suivante : ni l'une ni l'autre ne repose sur des faits que l'établissement aurait lui-même constatés.

§1 — L'identification des risques

Les schémas de blanchiment recourant aux crypto-actifs sont désormais documentés par les autorités (A). Encore faut-il les traduire dans les instruments internes de l'établissement (B).

A. Les typologies de blanchiment en matière de crypto-actifs

Les schémas se distinguent selon qu'ils cherchent ou non à dissimuler le parcours des fonds, car cette distinction commande ce que l'établissement peut percevoir.

1. Les schémas de conversion directe

Dans une première série de situations, les fonds sont convertis sans dissimulation particulière : produit d'une escroquerie ou d'un rançongiciel converti auprès d'une plateforme puis viré, ou conversion par un particulier de ses avoirs.

L'établissement perçoit alors un virement en euros provenant d'une plateforme identifiée. Cette perception ne lui livre pas l'origine première des fonds, mais elle lui permet de conduire les diligences ordinaires : vérification de la cohérence de l'opération avec le profil du client, demande de justificatifs sur l'origine des avoirs, examen de la plateforme émettrice et de son statut. La situation, à ce stade, n'est pas fondamentalement différente de celle d'un virement reçu de tout établissement financier étranger.

Il faut noter que cette hypothèse est aussi celle où le dispositif européen produit son plein effet. Si la plateforme émettrice est agréée dans l'Union, elle a elle-même identifié son client, appliqué ses propres mesures de vigilance et transmis les informations requises. L'établissement bancaire opère alors comme second maillon d'une chaîne complète, et sa diligence consiste principalement à vérifier la cohérence de ce qu'il reçoit.

2. Les schémas d'opacification

D'autres techniques visent précisément à rompre la traçabilité : recours à un service de mixage, passage successif entre plusieurs chaînes, circulation en jetons adossés à une monnaie par portefeuilles auto-hébergés, ou conversion auprès d'une plateforme établie hors de l'Union suivie d'un virement depuis un compte étranger.

Ce qui distingue ces schémas des précédents se situe entièrement en amont, dans une partie du parcours que l'établissement ne perçoit pas. Et c'est là que réside la difficulté centrale du présent chapitre : le virement reçu peut présenter la même apparence dans les deux hypothèses. Un virement de cinquante mille euros provenant d'une plateforme européenne agréée, au bénéfice d'un client dont le profil le justifie, se présente à l'établissement sous une forme identique, que les crypto-actifs convertis proviennent d'une acquisition régulière ou qu'ils aient été préalablement mêlés dans un service de mixage puis reconvertis à plusieurs reprises.

Cette identité d'apparence a une conséquence juridique qu'il convient d'énoncer clairement. La vigilance de l'établissement ne peut pas s'exercer sur la seule opération qu'il observe, puisque celle-ci ne porte pas en elle-même la marque du risque. Elle suppose l'accès

à une information extérieure — soit celle qui accompagne le transfert au titre de la règle du voyage, soit celle que produit une analyse de la chaîne. L'obligation de vigilance a donc, pour ces flux, un objet que l'établissement ne peut atteindre par ses propres moyens ordinaires.

B. La traduction dans les dispositifs internes

L'identification des risques se concrétise par deux instruments, l'un statique, l'autre dynamique.

1. La classification des risques

L'établissement est tenu d'élaborer une classification des risques propre à son activité, tenant compte notamment des produits et services proposés, des caractéristiques de sa clientèle et des canaux de distribution utilisés. Cette classification est le fondement de l'approche par les risques : c'est elle qui détermine l'intensité des mesures de vigilance appliquées à chaque relation.

Cette classification ne procède pas de la seule appréciation de l'établissement. Les analyses de risques publiées par les autorités en constituent le point d'appui obligé : l'analyse nationale des risques établie par le Conseil d'orientation de la lutte contre le blanchiment[59], les analyses sectorielles publiées par l'Autorité de contrôle prudentiel et de résolution et par l'Autorité des marchés financiers, ainsi que, au niveau européen, l'évaluation supranationale des risques établie par la Commission[60] et les avis périodiques de l'Autorité bancaire européenne sur les risques affectant le secteur financier de l'Union[61].

Le rôle de ces documents mérite d'être précisé, car il est ambivalent. Ils fournissent à l'établissement la matière de sa propre analyse, et à ce titre ils remplissent une fonction indispensable. Mais ils la lui fournissent sous une forme déjà agrégée et qualifiée par l'autorité : lorsque l'analyse nationale des risques qualifie l'exposition d'un secteur, l'établissement n'est pas en position de contester cette qualification, qui devient de fait le

---

[59]COLB, *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, sept. 2019.
[60]Commission européenne, COM(2022) 554 final, 27 octobre 2022, et document de travail SWD(2022) 344 final.
[61]Autorité bancaire européenne, avis EBA/Op/2023/08 du 13 juillet 2023, faisant suite à l'avis EBA/Op/2021/04 du 3 mars 2021.

point de départ obligé de sa classification. La première pièce du dispositif interne repose ainsi, elle aussi, sur une appréciation exogène.

2. Les scénarios de surveillance des opérations

L'obligation de vigilance constante se traduit en pratique par des dispositifs automatisés qui détectent les opérations atypiques et génèrent des alertes, lesquelles sont ensuite examinées par des analystes.

Le degré de précision auquel la conformité de ces dispositifs est appréciée mérite d'être mesuré. Il ressort de la pratique décisionnelle que le manquement se caractérise au niveau des paramètres, et non à celui des principes : un dispositif automatisé de surveillance ne tenant pas compte de toutes les informations nécessaires à la détection des opérations atypiques, notamment les revenus et le patrimoine des clients, constitue une carence retenue par le superviseur, de même que l'accumulation d'alertes non traitées ou dont le traitement demeure inachevé sur une durée prolongée[62].

Cette observation est essentielle pour la suite du raisonnement. Elle signifie que l'obligation de vigilance, énoncée en termes généraux par la loi, se concrétise et se juge au niveau du paramétrage. Elle signifie aussi que l'établissement qui souhaite appréhender les flux d'origine crypto doit traduire un risque en scénarios de détection — c'est-à-dire en seuils, en critères et en règles de déclenchement — sans qu'aucun texte, aucune orientation et aucune décision ne lui indique quels seuils, quels critères et quelles règles seraient tenus pour adéquats.

L'Autorité de contrôle prudentiel et de résolution a par ailleurs documenté, dans un rapport de juillet 2025 consacré à la prévention des comptes rebonds, le fonctionnement d'un schéma voisin par sa structure. Elle y relève que les virements reçus identifiés a minima comme suspects ont représenté six cent soixante et un millions d'euros, en hausse de quarante-cinq pour cent par rapport à l'exercice précédent, pour cent trente-trois mille relations d'affaires récipiendaires contre cent un mille, treize organismes concentrant près de quatre-vingt-dix pour cent de ces virements[63]. Ce rapport n'a pas valeur contraignante, mais il indique les attentes du superviseur en matière de pilotage du dispositif, d'entrée en relation, de connaissance du client, de détection automatisée et d'examen renforcé.

---

[62] ACPR, commission des sanctions, décision n° 2024-02 du 19 juin 2025, Banque Delubac et Cie.
[63] ACPR, *Rapport sur la prévention des comptes rebonds*, 17 juillet 2025.

§2 — Les moyens mobilisés

Deux moyens principaux permettent à l'établissement de dépasser ce que le seul virement lui donne à voir : l'analyse des transactions inscrites sur la chaîne (A), et la vigilance exercée à l'égard des prestataires avec lesquels il entre en relation (B).

A. L'analyse des transactions inscrites sur la chaîne

Il convient d'exposer la fonction de ces outils avant d'examiner la place que le droit leur reconnaît.

1. Les outils et leur fonction

Les outils d'analyse transactionnelle permettent de suivre et d'analyser les flux de crypto-actifs sur une chaîne de blocs. Ils rattachent des adresses à des entités identifiées, regroupent celles qui paraissent relever d'un même détenteur, et attribuent à une adresse ou à une transaction un niveau de risque tenant compte de son historique. Ils sont utilisés tant par les régulateurs et les autorités répressives que par les prestataires et les établissements financiers.

L'Autorité de contrôle prudentiel et de résolution en a établi la nécessité en termes explicites : si les principales chaînes de blocs autorisent un certain niveau de transparence en permettant de consulter l'ensemble des transactions réalisées par les adresses du réseau, l'analyse de ces transactions et l'évaluation des risques requièrent des outils spécialisés et un temps d'investigation croissant en fonction de la complexité des chaînes de transaction[64].

Ces outils permettent ainsi à l'établissement d'accéder à une information que le virement ne lui livre pas, en remontant au-delà de la plateforme émettrice. Ils constituent, dans l'état actuel du droit, le seul moyen dont il dispose pour percevoir la différence entre les deux séries de schémas exposées plus haut.

2. Le renvoi du droit à des instruments privés

La particularité de ces outils tient à ce que le droit européen y renvoie lui-même, sans les régir.

---

[64]VASQUES (V.) et COTIER (J.-F.), art. préc.

Le règlement MiCA prévoit ainsi que les crypto-actifs dotés de fonctions d'anonymisation ne peuvent être admis à la négociation que si leur traçabilité est assurée, cette assurance pouvant être obtenue au moyen d'outils d'analyse transactionnelle[65]. La disposition est remarquable : elle subordonne une décision d'admission relevant du droit financier à l'emploi d'un instrument dont ni la conception, ni les méthodes, ni la mise à jour ne relèvent d'un cadre réglementaire.

Les orientations de l'Autorité bancaire européenne relatives aux facteurs de risque procèdent de la même logique. Adoptées le 16 janvier 2024 et applicables depuis le 30 décembre 2024, elles comportent, au-delà des développements consacrés aux prestataires eux-mêmes, des indications destinées aux établissements de crédit et financiers qui comptent de tels prestataires parmi leurs clients ou se trouvent exposés aux crypto-actifs, et elles envisagent le recours aux outils d'analyse de chaîne parmi les mesures d'atténuation[66].

Il faut mesurer la portée de cette configuration. La doctrine relève d'ailleurs, sans nécessairement en tirer les conséquences, que ce sont les travaux des sociétés d'analyse qui permettent de connaître avec un degré de précision relativement fin le montant des activités illicites recourant aux crypto-actifs, alors que de tels chiffres n'existent pas dans le secteur bancaire[67]. La connaissance du risque, la mesure du risque et l'instrument de détection du risque procèdent ainsi, pour ce segment d'activité, de sources privées. L'établissement demeure seul responsable de l'exécution de son obligation, mais les moyens de cette exécution lui échappent en grande partie.

B. La vigilance à l'égard des prestataires clients

Deux séries de règles encadrent cette relation, dont l'une est déjà applicable et l'autre le sera en 2027.

1. Les orientations européennes de janvier 2024

Les orientations précitées identifient les facteurs de risque à considérer dans la relation nouée avec un prestataire de services sur crypto-actifs. Au premier rang figurent l'existence

[65]Règlement (UE) 2023/1114, art. 76, § 3.
[66]Autorité bancaire européenne, orientations EBA/GL/2024/01 du 16 janvier 2024, modifiant les orientations EBA/GL/2021/02, applicables depuis le 30 décembre 2024.
[67]DE VAUPLANE (H.), « Lutte contre le blanchiment et crypto-actifs : un déséquilibre entre la protection des libertés fondamentales et la lutte contre la criminalité », *RD bancaire et fin.* 2025, dossier 42.

et la portée de l'agrément dont le prestataire est titulaire, la relation nouée avec un acteur non agréé au titre du règlement MiCA présentant un risque accru. Elles envisagent également les facteurs tenant aux transferts vers ou depuis des adresses auto-hébergées et ceux tenant à l'intervention de plateformes décentralisées.

Ces orientations présentent, pour la question examinée ici, une importance qui excède leur objet apparent. Elles constituent en effet le seul instrument de droit souple européen qui traite expressément de la situation de l'établissement bancaire exposé aux crypto-actifs sans être lui-même prestataire. Elles fournissent donc à cet établissement, sinon un standard, du moins une grille de lecture officiellement établie.

Leur portée doit cependant être appréciée avec exactitude. Elles énoncent des facteurs de risque, c'est-à-dire des éléments dont l'établissement doit tenir compte dans son appréciation ; elles n'énoncent pas de diligences déterminées, c'est-à-dire des actes qu'il devrait accomplir. La différence est décisive : un facteur de risque oriente une appréciation, il ne fournit pas une règle de conduite. Il faut ajouter que ces orientations relèvent désormais du mandat de l'autorité européenne de lutte contre le blanchiment, laquelle a repris au 1er janvier 2026 les compétences correspondantes de l'Autorité bancaire européenne, ce qui introduit un facteur supplémentaire d'instabilité normative.

2. Le régime de la correspondance transfrontalière

La relation entre une banque et un prestataire a été rattachée au régime des relations de correspondance. Ce rattachement, souvent présenté comme une construction interprétative suspendue à l'entrée en application du règlement de 2024, est en réalité déjà consacré en droit français.

Le décret du 23 décembre 2024 impose en effet, en cas de relation transfrontalière de correspondant impliquant l'exécution de services sur crypto-actifs, de vérifier au moment de nouer la relation d'affaires que l'entité cliente est agréée ou enregistrée ; il impose en outre de documenter et de consigner la décision lorsqu'il est mis fin à une telle relation pour des raisons liées à la politique de lutte contre le blanchiment[68]. Cette seconde obligation, dont la portée sera examinée à la section suivante, constitue le premier encadrement juridique de la décision de rupture.

[68]Décret n° 2024-1205 du 23 décembre 2024, préc.

Le règlement anti-blanchiment de 2024 consolidera ce rattachement en soumettant à des mesures de vigilance renforcée les relations de correspondance entre un prestataire établi dans l'Union et un organisme établi dans un pays tiers[69]. Ce texte ne produira toutefois ses effets qu'à compter du 10 juillet 2027.

Une réserve doit être formulée, car elle nuance le raisonnement sans le contredire. Le standard international opère une distinction que le droit européen ne reprend pas : le Groupe d'action financière précise que la vigilance à l'égard de la contrepartie exercée au titre de la règle du voyage est distincte des obligations applicables aux relations de correspondance transfrontalières[70]. Le rattachement opéré par le droit européen constitue donc un choix propre, et non la transposition d'un standard préexistant. Ce choix se comprend au regard de la structure du risque — la banque qui ouvre un compte à un prestataire lui donne accès au système de paiement, comme le ferait une relation de correspondance classique —, mais il devra être justifié plutôt que présumé.

Les établissements ne sont donc pas démunis face aux flux d'origine crypto. Tous les moyens qu'ils mobilisent ont toutefois ceci de commun qu'ils reposent sur des constatations opérées par d'autres : le prestataire en amont, l'analyste de chaîne, l'autorité qui publie une analyse de risques, le superviseur étranger. Reste à savoir au regard de quelle exigence cette vigilance de seconde main sera appréciée.

Section 2 — Une obligation mesurée à un standard indéterminé

Les dispositifs décrits ne valent que s'ils satisfont aux exigences au regard desquelles ils seront appréciés. Ces exigences relèvent du contrôle prudentiel, et elles présentent une particularité : elles ne figurent dans aucun texte, mais se forment par la pratique décisionnelle du superviseur. Encore faut-il savoir comment ce standard se construit, et ce qu'il en est s'agissant des flux d'origine crypto (§1). À cette indétermination s'ajoutent des limites tenant aux moyens eux-mêmes, dont la conjonction explique le recours à une solution d'évitement (§2).

[69]Règlement (UE) 2024/1624, préc. ; SABBAN (D.), art. préc., n° 11.
[70]GAFI, *Targeted Update*, juin 2023.

§1 — L'indétermination du standard de diligence

Il convient d'observer d'abord d'où procède ce standard et à quel niveau il s'exprime (A), avant de constater qu'il ne s'est pas formé s'agissant des flux d'origine crypto (B).

A. Un standard formé par la pratique décisionnelle

Ce standard ne figure dans aucun texte : il faut établir d'où il procède, puis à quel degré de détail il s'exprime.

1. Un référentiel construit par accumulation

Les obligations légales de vigilance sont volontairement ouvertes. Le Code monétaire et financier impose à l'établissement de connaître son client, d'exercer une vigilance constante sur les opérations et de déclarer ses soupçons, mais il ne fixe ni le contenu ni l'intensité de ces diligences, qui doivent être adaptées aux risques. Cette ouverture est le corollaire nécessaire de l'approche par les risques : une règle uniforme serait contradictoire avec l'exigence d'adaptation.

Il en résulte que le contenu concret de l'obligation ne se découvre pas à la lecture du texte, mais dans les instruments qui l'explicitent. Trois sources y concourent. Les décisions de la commission des sanctions d'abord, qui précisent au fil des espèces ce qui constitue un manquement. Les lignes directrices et principes d'application sectoriels publiés par le superviseur ensuite, au premier rang desquels les lignes directrices conjointes de l'Autorité de contrôle prudentiel et de résolution et de Tracfin relatives aux obligations de vigilance sur les opérations et aux obligations de déclaration, dont la version actualisée a été publiée le 23 avril 2025[71]. Les orientations européennes enfin, examinées plus haut.

Le référentiel se constitue ainsi par sédimentation, chaque décision ajoutant une précision à celles qui l'ont précédée. Cette méthode présente un avantage — elle permet une adaptation continue aux évolutions du risque — et un inconvénient qui est le revers exact de cet avantage : le référentiel ne préexiste pas au comportement qu'il sert à juger. L'assujetti connaît l'exigence après coup.

[71] ACPR et Tracfin, lignes directrices conjointes du 23 avril 2025.

2. Un référentiel exprimé au niveau des paramètres

Le degré de détail auquel ces exigences s'expriment mérite d'être précisément mesuré, car il détermine ce que l'établissement doit anticiper.

Les griefs retenus par la commission des sanctions ne portent pas sur des manquements de principe mais sur des défaillances de paramétrage. Une décision du 19 juin 2025, ayant donné lieu à un blâme et à une sanction pécuniaire de six cent mille euros, en fournit une illustration complète : le dispositif automatisé de surveillance ne tenait pas compte de toutes les informations nécessaires à la détection des opérations atypiques, dont les revenus et le patrimoine des clients ; le traitement des alertes était jugé défaillant, plusieurs dizaines de milliers d'alertes demeurant non traitées ou en cours, dont une part significative ouverte depuis plus de quatre mois ; les mesures de vigilance complémentaire et renforcée n'avaient pas été correctement mises en œuvre ; des comptes avaient été clôturés pour un motif tiré de la lutte contre le blanchiment sans qu'un examen renforcé ait été conduit ni qu'une déclaration de soupçon ait été adressée[72].

Deux enseignements doivent être tirés de cette pratique.

Le premier tient au niveau auquel le manquement se caractérise. Ce n'est pas l'absence de dispositif qui est sanctionnée, mais son inadéquation technique : les informations qu'il exploite, les scénarios qu'il applique, les délais dans lesquels les alertes sont traitées. L'obligation de vigilance, énoncée en termes généraux, se juge au niveau du réglage.

Le second, plus significatif encore pour le présent propos, tient à ce que ces exigences supposent une antériorité. Un dispositif de surveillance fonctionne par comparaison entre une opération et un profil ; il détecte l'atypique par rapport à un typique préalablement établi. Une relation d'affaires récente ne fournit pas cette base de comparaison, ce qui constitue une limite structurelle et non organisationnelle. Or le rapport précité de l'Autorité de contrôle prudentiel et de résolution relève précisément que les comptes utilisés comme comptes de transit sont le plus souvent de création récente. La détection par comparaison est ainsi la moins opérante là où le risque est le plus élevé.

[72]ACPR, commission des sanctions, décision n° 2024-02 préc.

B. Son silence sur les flux d'origine crypto

Deux séries d'observations s'imposent, l'une portant sur les questions que ces flux soulèvent, l'autre sur l'état de leur traitement.

1. Les questions techniques non tranchées

Les interrogations propres aux flux d'origine crypto ne trouvent réponse ni dans les textes, ni dans les orientations disponibles, ni dans la pratique décisionnelle. Elles peuvent être formulées avec précision, et cette précision même fait apparaître l'étendue de la lacune.

Quelle profondeur d'analyse de la chaîne un établissement doit-il conduire ? La question n'est pas théorique : remonter d'un transfert à l'origine des fonds suppose de parcourir un nombre variable de transactions successives, et rien n'indique où cette remontée doit s'arrêter. Quelle valeur accorder à un score de risque fourni par un prestataire d'analyse, et faut-il le corroborer par d'autres moyens ? Quel niveau d'examen appliquer à un prestataire candidat à l'entrée en relation, au-delà de la vérification de son agrément que le décret du 23 décembre 2024 impose ? Que doit faire l'établissement lorsque l'information transmise au titre de la règle du voyage lui paraît incomplète, alors qu'il n'est pas en mesure de savoir si cette incomplétude tient à une défaillance de la contrepartie ou à une limite technique de l'outil employé ?

Ces questions se posent toutes au niveau opérationnel, c'est-à-dire précisément à celui auquel les manquements se caractérisent. L'établissement se trouve ainsi dans une situation qu'il faut nommer : il sait que sa conformité sera jugée au niveau du paramétrage, et il ne dispose d'aucune indication sur le paramétrage attendu.

2. L'absence de pratique décisionnelle

Aucune décision de la commission des sanctions n'est intervenue à ce jour sur ces questions.

Cette absence appelle la même prudence que celle relevée à propos des prestataires : elle peut tenir à la jeunesse du phénomène, à des procédures en cours, ou à l'orientation des contrôles vers d'autres sujets. Elle ne saurait s'interpréter comme une tolérance du superviseur, et l'établissement qui en tirerait une telle conclusion s'exposerait précisément au risque qu'elle recouvre.

Elle produit néanmoins un effet certain sur la situation des assujettis, et cet effet constitue le cœur de la démonstration du présent mémoire. Le référentiel applicable aux flux d'origine crypto se constituera nécessairement après les faits qu'il servira à apprécier. L'établissement doit donc, aujourd'hui, régler ses dispositifs selon des critères dont il apprendra ultérieurement s'ils étaient adéquats. Cette configuration est inhérente à tout référentiel formé par accumulation, mais elle atteint ici un degré particulier : là où, pour les flux classiques, l'établissement dispose de trois décennies de pratique décisionnelle et de typologies publiées par la cellule de renseignement financier, il ne dispose, pour les flux d'origine crypto, d'aucun précédent.

Il en résulte que l'obligation de vigilance conserve, pour ces flux, la seule forme que la loi lui donne : une obligation de moyens adaptés au risque, dont ni les moyens ni l'adaptation ne sont spécifiés. Ce n'est pas une carence rédactionnelle qu'il faudrait imputer au législateur ; c'est la conséquence du fait que le standard, dans cette matière, ne se forme pas par le texte mais par la décision, et qu'aucune décision n'est encore intervenue.

§2 — Les limites tenant aux moyens et leurs conséquences

Les moyens exposés à la section précédente permettent à l'établissement de dépasser ce que le seul virement lui donne à voir. Ils comportent toutefois des limites qui leur sont propres. Les premières tiennent à ce que l'analyse est externalisée (A) ; les secondes tiennent à la solution d'évitement que la conjonction de ces difficultés rend rationnelle (B).

A. Les limites de l'analyse externalisée

Il convient d'examiner la nature du renvoi opéré par le droit avant la portée juridique des résultats obtenus.

1. Une exigence réglementaire renvoyée à des instruments privés

Le constat établi à la section précédente doit ici être analysé dans ses conséquences juridiques. Le droit européen conditionne certaines décisions à l'emploi d'outils d'analyse transactionnelle et envisage leur usage parmi les mesures d'atténuation des risques, sans définir ces outils, sans en fixer les exigences de qualité et sans soumettre leurs concepteurs à une quelconque obligation.

Il en résulte une configuration singulière au regard des principes du droit de la conformité. L'établissement demeure seul débiteur de l'obligation et seul justiciable devant le superviseur. Mais la satisfaction de cette obligation dépend d'un instrument dont il n'a pas la maîtrise : il ne connaît ni les méthodes d'attribution des adresses, ni les critères de notation du risque, ni le rythme de mise à jour des bases employées. Il ne peut donc ni auditer l'outil, ni en garantir les résultats, ni opposer au superviseur une défaillance de celui-ci.

Le contraste mérite d'être relevé avec les flux classiques. Pour ceux-ci, la fonction d'orientation de la vigilance est assurée par des typologies publiées par la cellule de renseignement financier et par les analyses de risques des autorités : elles émanent d'une autorité publique, elles sont accessibles, elles peuvent être discutées. Pour les flux d'origine crypto, cette fonction est en grande partie assurée par des instruments privés. Le déplacement n'est pas neutre : il transfère à des opérateurs de marché une part de la définition pratique de ce que la vigilance exige.

2. La portée juridique indéterminée de leurs résultats

La recevabilité de l'analyse de la chaîne devant le juge pénal, établie au premier chapitre, ne dit rien de ce qui est attendu d'un assujetti au titre de sa vigilance. Ce sont deux questions distinctes, et leur confusion serait une erreur de méthode : le juge répressif apprécie une preuve, le superviseur apprécie une diligence.

Trois questions demeurent ouvertes, et leur formulation suffit à en montrer la portée. Un score de risque peut-il fonder à lui seul une décision affectant le client — refus d'exécution, examen renforcé, déclaration de soupçon —, ou appelle-t-il un examen complémentaire dont la consistance resterait à définir ? La production d'une telle analyse constitue-t-elle une diligence attendue ou une simple faculté ? Et, question la plus délicate, l'obligation de se doter de moyens adaptés au risque peut-elle conduire à apprécier les dispositifs d'un établissement au regard de l'existence de tels outils sur le marché, de sorte que le fait de ne pas en disposer constituerait en soi un manquement ?

Cette dernière question mérite un développement, car elle illustre le mécanisme qui traverse tout le présent chapitre. Si la réponse est affirmative, l'exigence réglementaire se trouve définie par l'état de l'offre commerciale : ce que le marché propose devient ce que le droit exige. Si elle est négative, l'établissement qui s'abstient de recourir à ces outils satisfait à son obligation tout en demeurant aveugle à la part du risque que seule l'analyse de chaîne

permet de percevoir. Aucune de ces deux branches n'est satisfaisante, et aucune n'est aujourd'hui tranchée.

B. Le dérisquage comme solution d'évitement

Le phénomène doit être établi et son encadrement exposé, avant que ses effets soient appréciés.

1. Un phénomène documenté et désormais encadré

Les difficultés d'accès aux services bancaires rencontrées par les acteurs du secteur des crypto-actifs sont documentées. La doctrine relève que les entreprises françaises du secteur s'exposent à de nombreux refus d'ouverture de comptes de dépôt ainsi qu'à des résiliations unilatérales de la part des établissements de crédit, ces réticences s'expliquant par les contraintes tenant à la lutte contre le blanchiment[73]. Le constat avait été établi dès 2021 par un groupe de travail réuni au sein du Forum Fintech, associant les autorités de supervision et les représentants du secteur[74].

L'Autorité bancaire européenne en a conduit l'analyse la plus complète dans un avis consacré au dérisquage. Elle y retient que si les décisions de ne pas nouer ou de rompre une relation d'affaires, ou de ne pas exécuter une opération, peuvent être conformes au cadre européen de lutte contre le blanchiment, le dérisquage de catégories entières de clients, sans considération des profils de risque individuels, peut être injustifié et constituer le signe d'une gestion inefficace du risque[75]. Cet avis n'est pas resté sans suite : à la demande de la Commission européenne, l'Autorité a adopté le 31 mars 2023 des orientations relatives aux politiques et contrôles permettant une gestion efficace des risques lors de la fourniture d'un accès aux services financiers, qui clarifient l'articulation entre cet accès et les obligations de vigilance, énoncent que plusieurs options doivent être envisagées avant toute décision de rejet, et fixent les étapes à suivre lorsqu'un établissement envisage de refuser ou de rompre une relation d'affaires pour des motifs tirés du risque de blanchiment[76].

---

[73]GUILLEBON (T.), « L'adaptation du droit français au nouveau statut de prestataire de services sur crypto-actifs (PSCA) », *RD bancaire et fin.* 2025, dossier 9.

[74]Forum Fintech ACPR-AMF, rapport du groupe de travail sur l'accès des PSAN aux comptes bancaires, 2021.

[75]Autorité bancaire européenne, *Opinion on de-risking*, EBA/Op/2022/01.

[76]Autorité bancaire européenne, orientations EBA/GL/2023/04 du 31 mars 2023 ; voir également les orientations EBA/GL/2023/03 de la même date.

Le règlement (UE) 2024/1624, non encore applicable mais annonciateur de l'état du droit à venir, prolonge cette préoccupation sous un autre angle. Il encadre les partenariats de partage d'informations entre entités assujetties en visant explicitement le risque que de tels échanges conduisent à des refus ou à des ruptures de relation d'affaires discriminatoires à l'égard de personnes figurant sur des listes partagées, et il impose à chaque entité assujettie de conduire sa propre évaluation du risque de blanchiment avant toute décision de cette nature[77].

Le droit français a suivi une trajectoire parallèle. L'ordonnance du 15 octobre 2024 a renforcé le dispositif de droit au compte applicable aux prestataires de services sur crypto-actifs. L'article L. 312-23, II du Code monétaire et financier énonce désormais qu'un établissement de crédit ne refuse d'ouvrir un compte de dépôt que dans les cas énumérés par la loi, ce qui constitue une dérogation significative à la liberté contractuelle du banquier : là où celui-ci conservait le droit de refuser sous réserve de motifs objectifs et non discriminatoires, il se voit désormais imposer une obligation de contracter. Deux exceptions sont ménagées : l'impossibilité de satisfaire aux obligations de vigilance, et le cas où le demandeur ou son modèle économique présente un profil de risque excessif. Un nouveau IV impose en outre un préavis minimal de deux mois en cas de résiliation à l'initiative de l'établissement[78]. À quoi s'ajoute l'obligation, issue du décret du 23 décembre 2024, de documenter et de consigner la décision de mettre fin à une relation de correspondance pour des raisons tirées de la politique de lutte contre le blanchiment.

Le dérisquage n'est donc plus un comportement libre : il est devenu une décision juridiquement encadrée, dont les motifs sont limitativement énumérés et dont la mise en œuvre est soumise à des exigences de procédure et de motivation.

2. Un procédé contraire à sa finalité

Reste à apprécier les effets de ce procédé, et à comprendre les raisons de sa persistance malgré l'encadrement qui vient d'être décrit.

---

[77]Règlement (UE) 2024/1624, art. 75, § 4, c) et d) ; MEDJAOUI (K.), « Points clés de la réforme du nouveau cadre européen de la lutte contre le blanchiment d'argent et le financement du terrorisme (paquet AML6) », *RD bancaire et fin.* 2025, n° 1, prat. 2, p. 100.

[78]C. mon. fin., art. L. 312-23, II et IV, dans leur rédaction issue de l'ordonnance n° 2024-936 du 15 octobre 2024 ; BONNEAU (Th.), « L'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs », *RD bancaire et fin.* 2024, étude 12 ; GUILLEBON (T.), art. préc.

Le dérisquage s'explique par un faisceau de facteurs qu'il serait imprudent de réduire à un seul : incertitude sur les attentes réglementaires, coût de la conformité rapporté au volume d'affaires, aversion commerciale pour un secteur jugé peu rentable, considérations de réputation. Il faut toutefois observer que le premier de ces facteurs est celui que les développements qui précèdent ont établi. Un établissement sommé d'apprécier un risque sans disposer du référentiel qui lui indiquerait le niveau de diligence attendu, et dont la conformité sera jugée au niveau du paramétrage, adopte un comportement rationnel en s'abstenant. Le dérisquage n'est pas, dans cette perspective, une défaillance individuelle : c'est la réponse prévisible à une indétermination.

Ce constat est corroboré par une observation indépendante. La Cour des comptes relève qu'aucune étude n'a jamais mesuré les coûts et les bénéfices du dispositif de lutte contre le blanchiment, alors même que les professions assujetties rencontrées se disent intéressées par une telle évaluation, notamment parce que certaines d'entre elles considèrent accomplir une mission au profit de l'État sans contrepartie[79]. L'établissement qui se dérobe à un segment de clientèle n'agit donc pas seulement sous l'effet d'une indétermination normative : il le fait sans disposer d'aucune mesure officielle du coût qu'impliquerait le choix inverse.

L'encadrement mis en place n'a d'ailleurs pas supprimé la difficulté, et la doctrine a identifié le point exact par lequel il peut être contourné : il est à craindre que le motif tiré du profil de risque excessif ne devienne le moyen d'échapper à l'interdiction du refus d'ouverture[80]. L'observation est fondée, car l'appréciation d'un profil de risque relève, par construction, de la classification que l'établissement élabore lui-même. L'exception légale renvoie ainsi à l'instrument dont l'établissement a la maîtrise, ce qui en limite structurellement la portée contraignante.

Or le résultat produit est contraire à la finalité poursuivie, et c'est par ce constat que le raisonnement se referme. Les flux écartés ne disparaissent pas : ils se déplacent vers des acteurs moins regardants, sortant du champ de vision de l'établissement comme de celui de son superviseur. L'exclusion soustrait ainsi à la surveillance ce qu'elle prétend en préserver. Et le mécanisme se boucle sur lui-même : la technique de la régulation par les intermédiaires,

---

[79]Cour des comptes, *L'évolution du dispositif français de lutte contre le blanchiment de capitaux — Exercices 2012-2022*, févr. 2023, spéc. p. 52 : « les coûts et bénéfices associés à la lutte contre le blanchiment n'ont fait l'objet d'aucune étude », alors que « certaines professions assujetties estiment qu'elles effectuent une mission au profit de l'État sans contrepartie ».

[80]GUILLEBON (T.), art. préc., n° 52.

en laissant indéterminée l'obligation du dernier intermédiaire, conduit celui-ci à se retirer, et ce retrait rompt à son tour la chaîne dont dépendait le dispositif tout entier.

> *Les établissements ont développé des dispositifs qui leur permettent d'appréhender une part substantielle du risque. Ces dispositifs se heurtent toutefois à des limites qui tiennent moins à leur conception qu'à leur environnement juridique : indétermination du standard au regard duquel ils seront appréciés, dépendance à des instruments dont la portée n'est pas fixée, et recours à l'exclusion lorsque l'appréciation individuelle paraît hors de portée. La difficulté n'est donc pas que la banque manque de moyens : c'est que le droit ne lui dit pas ce qu'il attend de leur emploi.*

CONCLUSION GÉNÉRALE

Le dispositif européen de prévention du blanchiment appliqué aux crypto-actifs repose sur une technique unique, qui en constitue à la fois la force et la limite : la régulation des intermédiaires.

Cette technique n'a pas été choisie par défaut. Elle procède d'un raisonnement cohérent, exposé au premier chapitre : l'écosystème des crypto-actifs, conçu pour se passer d'intermédiaires, en a suscité de nouveaux, et les registres sur lesquels il repose sont transparents. Réguler l'infrastructure aurait été sans objet quant à la traçabilité, qui existe déjà ; l'enjeu portait sur les conditions d'attribution d'une adresse à une personne, c'est-à-dire sur les points de contact entre la chaîne et le monde des identités civiles. Le législateur européen a donc étendu à ces points de contact une méthode éprouvée depuis 1991, celle de la délégation de surveillance aux professionnels qui traitent les flux.

Le dispositif qui en résulte est cohérent et, dans une large mesure, opérant. Il identifie des acteurs, leur assigne des obligations, se dote d'un instrument de traçabilité juridique et institue une supervision européenne. Pour l'établissement bancaire, il produit un effet concret : il transforme une qualité de fait, invérifiable, en un statut juridique vérifiable, et il fait circuler avec l'opération une information que le registre ne fournit pas.

Mais cette technique porte en elle ses propres limites, et le premier chapitre a montré qu'elles ne sont pas accidentelles. Une régulation qui saisit des personnes est impuissante là où il n'y a pas de personne à saisir : la finance décentralisée en fournit l'illustration la plus nette, et l'exclusion dont elle bénéficie n'est pas un oubli mais une conséquence logique. Une régulation territoriale est impuissante là où l'acteur se situe hors de sa portée, et les données du Groupe d'action financière établissent qu'une minorité seulement des juridictions évaluées applique effectivement le standard international. Une obligation de transmission ne vaut, enfin, que ce que vaut la chaîne de ceux qui transmettent : les défaillances techniques et l'inégale application entre juridictions dégradent l'information avant qu'elle ne parvienne à son destinataire final. Le déplacement le plus récent est à cet égard significatif : la règle du voyage est désormais adoptée presque partout, mais son respect n'est presque nulle part contrôlé.

Ces limites ne suppriment pas le risque : elles le déplacent. Il se présente, en fin de parcours, à l'établissement bancaire, qui se trouve être, dans nombre d'hypothèses, le premier assujetti à le rencontrer.

Le second chapitre a montré la position dans laquelle cette technique le place. L'établissement dispose de moyens réels — classification des risques, scénarios de surveillance, analyse de la chaîne, vigilance à l'égard des prestataires clients — mais tous ont ceci de commun qu'ils reposent sur des constatations opérées par d'autres. Sa vigilance est une vigilance de seconde main, exercée sur des faits qu'il n'a pas constatés, au moyen d'instruments qu'il ne maîtrise pas, à partir d'analyses de risques qu'il n'a pas établies.

À cette dépendance s'ajoute une indétermination. Le standard au regard duquel sa conduite sera jugée ne figure dans aucun texte : il se forme par accumulation, au fil des décisions du superviseur, et il s'exprime au niveau des paramètres. Or aucune décision n'est intervenue s'agissant des flux d'origine crypto. L'établissement doit donc régler ses dispositifs selon des critères dont il apprendra ultérieurement s'ils étaient adéquats, dans une matière où il ne dispose d'aucun précédent.

La réponse à la question posée en introduction peut alors être formulée. La technique de la régulation par les intermédiaires demeure opérante aussi longtemps que la chaîne de ces intermédiaires est continue : dans cette hypothèse, l'établissement bancaire n'est que le second maillon d'un dispositif qui a déjà fonctionné, et sa vigilance consiste à vérifier la cohérence de ce qu'il reçoit. Elle cesse en revanche de guider sa conduite là où cette chaîne est rompue : il devient alors le seul point de contrôle, sans que la technique employée lui indique ce qui est attendu de lui. Le dispositif est donc le moins prescriptif là où il est le plus nécessaire.

De cette configuration procède le dérisquage, qui n'est pas une défaillance individuelle mais la réponse rationnelle d'un assujetti sommé d'apprécier un risque sans référentiel. Le droit européen et le droit français l'ont encadré — avis et orientations de l'Autorité bancaire européenne, droit au compte renforcé, obligation de documenter les décisions de rupture — , mais cet encadrement laisse subsister un motif dont l'appréciation relève de l'établissement lui-même. Or l'exclusion produit un résultat contraire à sa finalité : les flux écartés se déplacent vers des acteurs moins regardants. Le mécanisme se referme sur lui-même, l'indétermination de l'obligation du dernier intermédiaire conduisant à son retrait, et ce retrait rompant à son tour la chaîne dont dépendait le dispositif.

Mais une perspective se dessine : il s'agit de celle de l'achèvement du dispositif. Le règlement anti-blanchiment s'appliquera le 10 juillet 2027, les normes techniques qui doivent en préciser les obligations sont en cours d'élaboration, et la supervision directe de l'autorité européenne débutera le 1er janvier 2028. Une part de l'indétermination constatée tient au caractère inachevé de l'édifice, et il n'est pas exclu qu'elle se résorbe. Encore faut-il observer que les normes techniques attendues portent sur les obligations de vigilance en général, non sur les flux d'origine crypto en particulier, et que rien n'indique qu'elles trancheront les questions opérationnelles recensées au second chapitre.

BIBLIOGRAPHIE

1. Traités et manuels

BONNEAU (Th.), *Régulation bancaire et financière européenne et internationale*, Bruylant, 7e éd., 2024.

DRUMMOND (F.), *Droit financier : les institutions, les activités, les abus de marché*, Economica, 2020.

FLEURET (F.), LOURIMI (A.) et O'RORKE (W.), *Droit des crypto-actifs*, LexisNexis, 2e éd., 2024.

LASSERRE CAPDEVILLE (J.), STORCK (M.), MIGNOT (M.) et al., *Droit bancaire*, Dalloz, 4e éd., 2024.

LEGEAIS (D.), Blockchain et crypto-actifs, LexisNexis, 3e éd., 2025.

STOUFFLET (J.) et ROUAUD (A.-C.), *Droit bancaire*, LexisNexis, 10e éd., 2023.

2. Ouvrages, encyclopédies et fascicules

LEGEAIS (D.), « Régime juridique des crypto-actifs », *JurisClasseur Commercial*, fasc. 536.

O'RORKE (W.) et NIN (A.), « Prestataires de services sur crypto-actifs », *JurisClasseur Droit bancaire et financier*, fasc. 2505.

3. Articles

BARRET (N.), « Crypto-actifs et blanchiment, de faux amis », *RD bancaire et fin.* 2025, n° 6, dossier 44.

BONNEAU (Th.), « L'ordonnance n° 2024-936 du 15 octobre 2024 relative aux marchés de crypto-actifs », *RD bancaire et fin.* 2024, étude 12.

BONNEAU (Th.), « La réforme européenne 2024 du dispositif LCB-FT », *RD bancaire et fin.* 2025, dossier 26.

BONNEAU (Th.), « Le rôle des autorités de régulation », *RD bancaire et fin.* 2025, n° 2, dossier 12.

CLÉMENT (S.) et LELIEUR (J.), « La conformité anti-blanchiment face aux crypto-actifs », *RSC* 2021, n° 1, p. 15 et s.

DE VAUPLANE (H.), « Lutte contre le blanchiment et crypto-actifs : un déséquilibre entre la protection des libertés fondamentales et la lutte contre la criminalité », *RD bancaire et fin.* 2025, n° 6, dossier 42.

GUILLEBON (T.), « L'adaptation du droit français au nouveau statut de prestataire de services sur crypto-actifs (PSCA) », *RD bancaire et fin.* 2025, n° 2, dossier 9.

LASSERRE CAPDEVILLE (J.), « L'AMLA et les autres autorités européennes », *RD bancaire et fin.* 2025, dossier 29.

LEGEAIS (D.), « Loi narcotrafic et blanchiment de crypto-actifs », *RD bancaire et fin.* 2025, comm. 85.

LEGEAIS (D.), « Pratique des comptes de rebonds », *RD bancaire et fin.* 2025, comm. 115.

LE GUEN (J.), « La conservation des crypto-actifs à l'épreuve de l'ordonnance MiCA : entre continuité et rupture », *RD bancaire et fin.* 2025, n° 2, dossier 10.

LEROY (Y.), « La notion d'effectivité du droit », *Droit et société*, 2011/3, n° 79, p. 715-732.

LE TOUZÉ (M.), « La réforme du devoir de vigilance dans le paquet européen LCB-FT », *RD bancaire et fin.* 2025, dossier 31.

LYON LYNCH (O.), « L'AMLA/ALBC et le secteur financier », *RD bancaire et fin.* 2025, n° 5, dossier 27.

MEDJAOUI (K.), « Points clés de la réforme du nouveau cadre européen de la lutte contre le blanchiment d'argent et le financement du terrorisme (paquet AML6) », *RD bancaire et fin.* 2025, n° 1, prat. 2.

PAILLER (P.), « Blanchiment et crypto-actifs : le cadre réglementaire national et européen », *RD bancaire et fin.* 2025, n° 6, dossier 41.

SABBAN (D.), « Réglementation LCB-FT et crypto-actifs : des enjeux éminents, des défis persistants », *RD bancaire et fin.* 2025, n° 6, dossier 43.

VASQUES (V.) et COTIER (J.-F.), « La LCB-FT au cœur de la sécurité des services sur actifs numériques », *Revue Banque*, janv. 2024.

4. Rapports et avis

ADAN et Ipsos, *Baromètre de l'adoption des crypto-actifs*, janvier 2026.

ACPR, *Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme*, juin 2023.

ACPR, *Rapport sur la prévention des comptes rebonds pour le blanchiment d'escroqueries et autres fraudes*, 17 juillet 2025.

ACPR et Tracfin, *Lignes directrices conjointes relatives aux obligations de vigilance sur les opérations et aux obligations de déclaration et d'information à Tracfin*, 23 avril 2025.

AMF, *Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme*, juin 2024.

Autorité bancaire européenne, *Opinion on de-risking*, EBA/Op/2022/01.

Autorité bancaire européenne, avis sur les risques de blanchiment de capitaux et de financement du terrorisme affectant le secteur financier de l'Union, EBA/Op/2021/04, 3 mars 2021.

Autorité bancaire européenne, avis sur les risques de blanchiment de capitaux et de financement du terrorisme affectant le secteur financier de l'Union, EBA/Op/2023/08, 13 juillet 2023, accompagné du rapport EBA/REP/2023/21.

Autorité bancaire européenne, orientations modifiant les orientations EBA/GL/2021/02 en ce qui concerne les organisations à but non lucratif, EBA/GL/2023/03, 31 mars 2023.

Autorité bancaire européenne, *Orientations sur les facteurs de risque de blanchiment de capitaux et de financement du terrorisme*, EBA/GL/2021/02.

Autorité bancaire européenne, *Guidelines on policies and controls for the effective management of ML/TF risks when providing access to financial services*, EBA/GL/2023/04, 31 mars 2023.

Autorité bancaire européenne, *Orientations modifiant les orientations EBA/GL/2021/02 sur les facteurs de risque*, EBA/GL/2024/01, 16 janvier 2024.

Autorité bancaire européenne, *Orientations sur les exigences en matière d'information concernant les transferts de fonds et certains transferts de crypto-actifs*, EBA/GL/2024/11, 4 juillet 2024.

Autorité bancaire européenne et Autorité européenne des marchés financiers, *Joint report on recent developments in crypto-assets (Article 142 of MiCAR)*, EBA/Rep/2025/01 – ESMA75-453128700-1391, janvier 2025.

Autorité européenne des marchés financiers, *Orientations relatives à la sollicitation inversée au titre du règlement MiCA*, ESMA35-1872330276-2030, 26 février 2025.

Autorité européenne des marchés financiers, *Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*, ESMA75-453128700-1323, 17 décembre 2024.

Autorités européennes de surveillance, *Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets*, JC 2024 28, 10 décembre 2024.

Chainalysis, *Crypto Crime Report*, éditions 2025 et 2026.

COLB, *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, septembre 2019.

Commission européenne, *Rapport sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontières*, COM(2022) 554 final, 27 octobre 2022.

Commission européenne, *Proposition de règlement modifiant le règlement (UE) 2023/1114*, COM(2025) 943 final, 4 décembre 2025.

Cour des comptes, *L'évolution du dispositif français de lutte contre le blanchiment de capitaux — Exercices 2012-2022*, février 2023.

Finanstilsynet, *Principles for the assessment of decentralisation in the markets for crypto-assets*, 25 juin 2024.

Forum Fintech ACPR-AMF, *Rapport du groupe de travail sur l'accès des PSAN aux comptes bancaires*, 2021.

GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs*, éditions de juin 2022, juin 2023, juin 2024, juin 2025 et juillet 2026.

GAFI, *Best Practices in Travel Rule Supervision*, 2025.

5. Sites internet

Autorité bancaire européenne — www.eba.europa.eu

Autorité de contrôle prudentiel et de résolution — acpr.banque-france.fr

Autorité des marchés financiers — www.amf-france.org

Autorité européenne des marchés financiers — www.esma.europa.eu

EUR-Lex — eur-lex.europa.eu

Groupe d'action financière — www.fatf-gafi.org

Légifrance — www.legifrance.gouv.fr

TABLE DES MATIÈRES

REMERCIEMENTS 2

SOMMAIRE 3

LISTE DES ACRONYMES 4

INTRODUCTION 6

CHAPITRE 1 — LA RÉGULATION PAR LES INTERMÉDIAIRES, TECHNIQUE FONDATRICE DU DISPOSITIF EUROPÉEN 14

Section 1 — Le choix de l'intermédiation comme technique de prévention 14

§1 — Les fondements du choix régulatoire 15

A. Un écosystème réintermédiarisé et traçable **15**

1. La reconstitution d'intermédiaires identifiables **15**

2. La traçabilité des blockchains publiques 16

B. Une méthode éprouvée, étendue par étapes 17

1. La fonction de gardien du système financier 17

2. L'extension aux crypto-actifs de 2018 à 2024 18

§2 — Les instruments du cadre actuel 19

A. L'accès au marché et la traçabilité des transferts 20

1. MiCA et le statut des prestataires 20

2. Le règlement TFR et la règle du voyage 21

B. L'harmonisation des obligations et la supervision européenne 22

1. Le paquet anti-blanchiment de 2024 22

2. L'autorité européenne et le calendrier de mise en œuvre 23

Section 2 — Les angles morts de l'intermédiation 24

§1 — Les limites inhérentes au périmètre 25

A. Les acteurs hors d'atteinte 25

1. Les protocoles décentralisés sans opérateur 25

2. Les prestataires établis hors de l'Union 27

B. La circulation hors intermédiaire 28

1. Les portefeuilles auto-hébergés 28

2. Les techniques d'opacification et la réponse pénale 29

§2 — Les limites tenant à l'effectivité 30

A. La circulation imparfaite de l'information 30

1. Les limites techniques de la transmission 31

2. L'inégale application entre juridictions 31

B. La portée limitée du contrôle 32

1. Le déficit international de supervision 32

2. L'absence de contentieux disciplinaire national 33

CHAPITRE 2 — L'ÉTABLISSEMENT BANCAIRE, DÉBITEUR D'UNE VIGILANCE SANS RÉFÉRENTIEL CONSTITUÉ 35

Section 1 — Une vigilance construite sur une information exogène 35

§1 — L'identification des risques 35

A. Les typologies de blanchiment en matière de crypto-actifs 35

1. Les schémas de conversion directe 36

2. Les schémas d'opacification 36

B. La traduction dans les dispositifs internes 37

1. La classification des risques 37

2. Les scénarios de surveillance des opérations 38

§2 — Les moyens mobilisés 39

A. L'analyse des transactions inscrites sur la chaîne 39

1. Les outils et leur fonction 39

2. Le renvoi du droit à des instruments privés 39

B. La vigilance à l'égard des prestataires clients 40

1. Les orientations européennes de janvier 2024 40

2. Le régime de la correspondance transfrontalière 41
Section 2 — Une obligation mesurée à un standard indéterminé 42
§1 — L'indétermination du standard de diligence 43
A. Un standard formé par la pratique décisionnelle 43
1. Un référentiel construit par accumulation 43
2. Un référentiel exprimé au niveau des paramètres 44
B. Son silence sur les flux d'origine crypto 45
1. Les questions techniques non tranchées 45
2. L'absence de pratique décisionnelle 45
§2 — Les limites tenant aux moyens et leurs conséquences 46
A. Les limites de l'analyse externalisée 46
1. Une exigence réglementaire renvoyée à des instruments privés 46
2. La portée juridique indéterminée de leurs résultats 47
B. Le dérisquage comme solution d'évitement 48
1. Un phénomène documenté et désormais encadré 48
2. Un procédé contraire à sa finalité 49
CONCLUSION GÉNÉRALE 52
BIBLIOGRAPHIE 55
1. Traités et manuels 55
2. Ouvrages, encyclopédies et fascicules 55
3. Articles 55
4. Rapports et avis 57
5. Sites internet 59
TABLE DES MATIÈRES 60

Faculté de droit
de sciences politiques et de gestion
Université de Strasbourg

Résumé

La prévention du blanchiment repose depuis 1991 sur une technique constante : réguler des intermédiaires plutôt que des flux. Appliquée aux crypto-actifs par les règlements MiCA et TFR puis par le paquet de 2024, elle suppose des acteurs juridiquement saisissables et laisse donc subsister des situations qu'elle ne peut atteindre. L'établissement bancaire, qui n'exerce aucun service sur crypto-actifs, se trouve au point où ces flux redeviennent de la monnaie ayant cours légal. Ses dispositifs de vigilance sont réels, mais l'information dont ils dépendent est produite par d'autres, et le référentiel au regard duquel sa diligence sera appréciée ne s'est pas encore formé. La technique qui fait tenir le dispositif en amont est ainsi celle qui l'affaiblit en aval. Mots-clés : blanchiment de capitaux ; crypto-actifs ; MiCA ; règle du voyage ; devoir de vigilance ; dérisquage.

Résumé en anglais

Since 1991 the prevention of money laundering has relied on one constant technique: regulating intermediaries rather than flows. Applied to crypto-assets by the MiCA and TFR Regulations and the 2024 package, it presupposes legally identifiable actors and therefore leaves situations beyond its reach. The credit institution, providing no crypto-asset service, stands where such flows revert to legal tender. Its monitoring arrangements are real, but the information they depend on is produced by others, and the benchmark against which its diligence will be assessed has not yet emerged. The technique holding the framework together upstream is thus the one that weakens it downstream. Keywords: money laundering; crypto-assets; MiCA; travel rule; duty of vigilance; de-risking.