NOTE DE RECHERCHE

Libertés et souveraineté numérique

Collecter plus, protéger moins ?

Fuites de données, irréversibilité du préjudice et proportionnalité des obligations de collecte du cadre européen anti-blanchiment (AMLR / TFR)

Le cas des portefeuilles auto-hébergés de crypto-actifs

Avril 2026

INBi – www.inbi.fr

Synthèse

Le cadre européen anti-blanchiment (règlement AMLR[1], règlement TFR[2] et lignes directrices de l'ABE) impose aux prestataires de services sur crypto-actifs (CASP) un ensemble d'obligations de collecte de données d'identité, y compris la vérification des portefeuilles auto-hébergés au-delà de 1 000 €. Ces obligations créent mécaniquement des bases de données associant identités civiles et adresses cryptographiques.

La présente note établit trois constats empiriques. **Premier constat :** selon les principales sources d'analyse on-chain disponibles, l'activité illicite identifiée demeure minoritaire. Ces estimations, fondées sur des méthodologies propriétaires, constituent des ordres de grandeur plutôt que des mesures exhaustives. Ceci étant dit, le bénéfice et la proportionnalité d'une collecte systématique couvrant l'ensemble des utilisateurs restent à démontrer, une telle démonstration étant impérative sur le fondement de la Convention européenne des droits de l'Homme (CEDH)[3] et de la Charte des droits fondamentaux de l'Union européenne (CDFUE)[4]. **Deuxième constat :** les données liées à la détention de crypto-actifs (dénommés « actifs numériques » en droit français) sont structurellement irréversibles en cas de fuite. La fuite de la base de données e-commerce de Ledger en 2020 démontre empiriquement que même une fuite de données créant une inférence forte de détention produit des conséquences qui perdurent plus de cinq ans, alimentant phishing, extorsion et agressions physiques[5]. **Troisième constat :** la France concentre environ un quart des agressions physiques mondiales visant des détenteurs de crypto-actifs, avec un lien étayé entre centralisation de données et ciblage criminel[6] [7].

Ces constats trouvent un écho dans un audit institutionnel récent : le 11 mars 2026, la Cour des comptes néerlandaise (Algemene Rekenkamer) a conclu que les contrôles anti-blanchiment dans le secteur bancaire ont des « conséquences graves » pour les citoyens, que leurs « avantages restent inconnus », et qu'il existe des « indications de discrimination »[8].

Enfin, le standard international du GAFI n'impose pas une collecte uniforme : il repose sur une approche fondée sur les risques, renforcée depuis 2025 par la proportionnalité et les mesures

[1] Règlement (UE) 2024/1624 du 31 mai 2024 (AMLR). Applicable 10 juillet 2027.

[2] Règlement (UE) 2023/1113 du 31 mai 2023 (TFR). Applicable depuis le 30 décembre 2024.

[3] Voir par ex.CEDH, plen, Dudgeon c. Royaume-Uni, 22 octobre 1981, req. n° 7525/76, § 60 ; CEDH, ch., Crémieux c. France, 25 février 1993, apl. n° 11471/85, § 38.

[4] Voir par ex.CJUE, gr. ch., Digital Rights Ireland et Seitlinger e.a., 8 avril 2014, aff. jointes C-293/12 et C-594/12, § 49 ; CJUE, gr. ch., La Quadrature du Net et autres, 6 octobre 2020, aff. jointes C-511/18 et autres, § 131 ; Contrôleur européen à la protection des données, Avis sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE), 31 mai 2011, § 41 ; Groupe de travail article 29 sur la protection des données, Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif (WP 211), 27 février 2014, § 3.13-3.19.

[5] Ledger, Addressing the July 2020 e-commerce and marketing data breach, 29 juillet 2020 ; Ledger, Update on the data breach, 21 décembre 2020. CNIL, délibération SAN-2024-020 du 10 octobre 2024.

[6] CertiK, rapport 2025 : 72 agressions physiques vérifiées dans le monde ; la France en représente 19, soit 26,4 %.

[7] Affaire Ghalia C. (Bobigny) : selon la presse judiciaire, une agente des impôts mise en examen en juillet 2025 a utilisé ses accès fiscaux pour rechercher des investisseurs en cryptomonnaie et transmettre des informations à un réseau criminel.

[8] Algemene Rekenkamer (Cour des comptes néerlandaise), « Anti-money laundering checks: serious consequences for citizens, unknown benefits », 11 mars 2026.

simplifiées[9]. Au regard de la jurisprudence de la Cour européenne des droits de l'Homme (Cour EDH) et de la Cour de justice de l'Union européenne (CJUE) sur la conservation généralisée des données et le principe de minimisation, lequel est également imposé par le Règlement général sur la protection des données (RGPD), la présente note soulève la question de la proportionnalité des nouvelles obligations de collecte ; non seulement telles que le texte les impose, mais telles que l'architecture d'incitations pousse les acteurs privés à les appliquer. En transférant aux CASP l'évaluation du risque dans un cadre où la sous-conformité est sanctionnée mais la surcollecte ne l'est pas, le dispositif crée une incitation structurelle à la prudence défensive.

Le rapport prévu à l'article 37(2) du TFR (échéance : 1er juillet 2026) constitue la fenêtre réglementaire pertinente pour intégrer cette analyse.

1. Question de recherche

Question principale : Les obligations de collecte centralisée de données personnelles imposées par le cadre européen anti-blanchiment (AMLR et TFR) aux CASP satisfont-elles le test de nécessité et de proportionnalité qu'imposent la CEDH et la CDFUE, au regard (i) de la part démontrée des transactions illicites dans le volume total, (ii) de l'irréversibilité du préjudice en cas de fuite de données crypto-financières, (iii) du lien documenté entre centralisation de données et ciblage physique des détenteurs, (iv) de l'approche fondée sur les risques que le GAFI érige lui-même en standard international, et (v) des effets prévisibles de la délégation de l'évaluation du risque aux acteurs privés lorsqu'elle incite structurellement à la surconformité, à la surcollecte et à la prudence défensive ?

2. Cadre juridique

2.1. Les trois strates du cadre AMLR/TFR

Le dispositif européen s'articule en trois strates réglementaires distinctes.

Première strate : la vigilance à l'égard de la clientèle (CDD). Le règlement anti-blanchiment (AMLR, règlement (UE) 2024/1624), applicable à compter du 10 juillet 2027, érige les CASP (équivalent européen des PSAN français, « prestataires de services sur actifs numériques ») en entités assujetties. Le seuil de CDD (« Customer Due Diligence ») complète est fixé à 1 000 € pour les CASP[10], nettement inférieur au seuil général de 10 000 € applicable aux autres entités.

Deuxième strate : la travel rule. Le règlement sur les transferts de fonds (TFR, règlement (UE) 2023/1113), applicable depuis décembre 2024, impose aux CASP de transmettre avec chaque transfert les informations d'identité du donneur d'ordre et du bénéficiaire, sans seuil minimum.

[9]FATF, « FATF updates Standards and consults on guidance to better promote financial inclusion », 25 février 2025. La Plénière de février 2025 a approuvé le remplacement de « commensurate » par « proportionate », défini comme « a measure or action that appropriately corresponds to the level of identified risk and effectively mitigates the risks ». Voir aussi FATF, Guidance on AML/CFT Measures and Financial Inclusion, juillet 2025.

[10]AMLR, art. 19. Le seuil général de CDD pour les transactions occasionnelles est de 10 000 €, sous réserve de seuils plus bas prévus pour certaines situations. Les CASP font l'objet d'un régime spécifique : 1 000 € pour les transactions occasionnelles, avec identification et vérification du client même en dessous de ce seuil.

Troisième strate : les obligations relatives aux portefeuilles auto-hébergés. Le TFR prévoit qu'au-delà de 1 000 €, le CASP doit prendre des mesures adéquates pour apprécier si l'adresse auto-hébergée est détenue ou contrôlée par son client. L'AMLR complète ce dispositif : l'article 40 impose aux CASP des politiques, procédures et contrôles internes spécifiques pour gérer les risques LBC/FT liés aux interactions avec les portefeuilles auto-hébergés. L'article 79, quant à lui, interdit aux CASP de tenir des comptes crypto anonymes ; cette interdiction ne vise pas les fournisseurs de portefeuilles matériels ou logiciels lorsqu'ils n'ont ni accès ni contrôle sur les crypto-actifs. Toutefois, chaque interaction CASP/portefeuille génère une entrée dans les systèmes du CASP, associant identité civile et adresse cryptographique.

2.2. Les exigences de nécessité et de proportionnalité (incluant le principe de minimisation)

Notre système juridique est tenu à deux exigences lorsqu'il est question de limiter les libertés des individus, en particulier leur droit à la vie privée et à la protection des données personnelles, droits protégés sous le visa des articles 7 et 8 de la CDFUE et de l'article 8 de la CEDH. Ces exigences sont celles de nécessité et de proportionnalité, imposées par les deux textes précités[11]. Le RGPD en reprend la substance, son article 5 (1)(c) imposant en particulier que les données collectées soient « limitées à ce qui est nécessaire », son article 25 imposant la protection des données dès la conception et par défaut.

2.2.1 La jurisprudence de la Cour EDH : une mesure limitant les libertés doit être minimisée dans ses impacts, et son besoin démontré

La Cour EDH a établi avec une grande précision les conditions dans lesquelles une mesure limitative de vie privée est acceptable dans une société démocratique. La notion de vie privée, pour la Cour, n'est pas limitée à un « cercle intime » mais est une « notion large (...) qui recouvre également l'intégrité physique et morale de la personne ».[12] Elle protège « le droit de vivre en privé, loin de toute attention non voulue »[13], les données concernées incluant les informations bancaires, peu importe que ces dernières soient sensibles ou non, même lorsqu'elles sont de nature professionnelles.[14] Lorsqu'est arbitrairement remise en cause la liberté de choix d'un individu, la Cour EDH considère que cette atteinte peut être de nature à atteindre sa dignité humaine.[15] Dans le même sens, la Cour constitutionnelle fédérale allemande a considéré que le droit à l'auto-détermination d'un individu, protégé sur le terrain de la dignité de la personne, pouvait être remis en cause par la perte de contrôle de cet individu sur ses données, sans qu'il ne puisse connaître de la pertinence de leur utilisation, entraînant des possibilités d'influence sur sa personne et une potentielle pression psychologique.[16]

[11]Ces deux exigences sont parfois désignées ensemble sous le seul terme de « nécessité » ou de « proportionnalité », car elles se chevauchent dans une certaine mesure : voir par ex. Contrôleur européen à la protection des données, Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, avril 2017, p. 6.

[12]Cour EDH, gr. ch., Denisov c. Ukraine, 25 septembre 2018, req. n° 76639/11, §95-96.

[13]Cour EDH, 5ème Sect., Khadija Ismayilova c. Azerbaïdjan, 10 janvier 2019, req. n° 65286/13, 57270/14, § 139.

[14]Cour EDH, 3ème Sect ., M.N. et autres c. San Marino, 7 juillet 2015, req. n° 28005/12, § 51.

[15]Sur cette question voir Estelle De Marco et al., Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law, éd. Verts/Ale au Parlement européen, février 2022, n° 11 p. 161 et s., https://extranet.greens-efa-service.eu/public/media/file/1/7487.

[16]Cour constitutionnelle fédérale allemande, 15 décembre 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, §145, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.

Selon la Cour EDH, l'exercice normal de la vie privée est la confidentialité et la liberté d'agir par défaut. Toute collecte et tout accès à une donnée de vie privée est une ingérence en elle-même, et une ingérence distincte des autres accès et collectes, peu important, là encore, que l'information soit sensible ou que la personne concernée en ait ou non subi un inconvénient.[17]

Les États parties à la CEDH ont non seulement l'obligation de s'abstenir de toute ingérence arbitraire, mais également l'obligation d'adopter des mesures conçues pour faire en sorte que la vie privée soit respectée dans la sphère des rapports entre les personnes entre elles, incluant les entreprises.[18]

Les ingérences sont évidemment possibles, mais pour ne pas être arbitraires, en d'autres termes pour être conformes à la CEDH, elles doivent poursuivre un objectif légitime, elles doivent être efficaces dans la poursuite de cet objectif[19], et elles doivent enfin être proportionnées à cet objectif.

Concernant particulièrement l'efficacité de la mesure, donc le besoin qu'il y a à la mettre en oeuvre pour répondre de manière appropriée à l'objectif, le Groupe « Article 29 » sur la protection des données, devenu le Comité européen à la protection des données, a retenu une liste non exhaustive de questions à se poser, à la lumière des affaires jugées par la Cour EDH :
- « La mesure vise-t-elle à résoudre un problème qui, si l'on ne s'en occupe pas, peut entraîner des dommages ou des conséquences préjudiciables pour la collectivité ou une partie de la collectivité ?
- Existe-t-il des éléments démontrant que la mesure peut atténuer ces conséquences ?
- Quelles sont les attitudes générales (sociétales, historiques ou politiques, etc.) de la collectivité à l'égard du problème en question ?
- Les avis spécifiques ou l'opposition éventuelle exprimés par la société à l'égard d'une mesure ou d'un problème ont-ils été suffisamment pris en compte ? ».[20]

Concernant en particulier la démonstration selon laquelle la mesure envisagée est de nature à répondre à l'objectif, elle doit « se trouver établie de manière convaincante »[21] et si une mesure est proposée « pour remédier au manque d'efficacité de mesures existantes, cela doit être clairement expliqué et prouvé »[22]. La justification doit être « solide et pouvoir résister à l'examen. Il faut donc que les mesures proposées se fondent sur des travaux étayés par des faits, des statistiques, des projections, etc. Tous ces éléments contribueront à faire en sorte que le critère des motifs pertinents et suffisants soit satisfait ».[23]

La notion de proportionnalité implique une minimisation de l'ingérence, laquelle ne doit pas aller « au-delà de ce qui est nécessaire pour atteindre le but légitime poursuivi »[24]. Ceci implique d'une part que les impacts de l'ingérence soient réduits au maximum, et, d'autre part, lorsque cette

[17]Cour EDH, ch., Leander c. Suède, 26 mars 1987, req. n° 9248/81, § 48 ; Cour EDH, gr. ch., Rotaru c. Roumanie, 4 mai 2000, req. n° 28341/95, § 46. ; .

[18]Cour EDH, ch., X et Y c. Pays-Bas, 26 mars 1985, req. n° 8978/80, § 23 ; Cour EDH, gr. ch., Bărbulescu c. Roumanie, 5 septembre 2017, req. n° 61496/08, § 108-111 ; Cour EDH, gr. ch., Von Hannover c. Allemagne (no. 2), req. n° 40660/08 et 60641/08, 7 février 2012, § 9.

[19]La Cour évoque un « besoin social impérieux », qui renvoie notamment à un devoir, pour l'État, de fournir « une justification suffisante » selon laquelle ne pas adopter la mesure en cause conduira à des impacts négatifs sur des individus à protéger ou à la collectivité : Cour EDH, Dudgeon c. Royaume-Uni, 22 octobre 1981, req. n° 7525/76, § 60. Voir aussi Groupe de travail article 29 sur la protection des données, Avis 01/2014 (WP 211) précité, § 3.13-3.19 et 3.31.

[20]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif (WP 211), 27 février 2014, § 3.19.

[21]Cour EDH, ch., Crémieux c. France, 25 février 1993, req. n° 11471/85, § 38.

[22]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 (WP 211) précité, 27 février 2014, §3.26.

[23]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 (WP 211) précité, § 6.1.

[24]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 précité, §3.20, se référant là encore à plusieurs arrêts de la Cour EDH.

minimisation est assurée, que les impacts résiduels n'excèdent pas les bénéfices de l'ingérence pour la société[25]. En particulier, l'ingérence doit être réduite au strict nécessaire sur les aspects suivants :

- Le nombre d'informations personnelles conservées et la durée pendant laquelle elles vont être traitées[26], le nombre de lieux et de personnes affectés[27]. En particulier, la conservation des données ne peut pas être de « nature indiscriminée » avant toute suspicion qu'une infraction a été commise.[28] En cas de suspicion préalable, la conservation ne peut pas avoir lieu « indépendamment de la nature ou de la gravité de l'infraction que la personne est soupçonnée d'avoir commise »[29].
- Les cas d'exercice de la mesure et le temps pendant lequel la mesure va être appliquée[30]. La Cour EDH vérifie également si le but poursuivi par l'ingérence peut être atteint de manière satisfaisante par des moyens moins intrusifs : « si une mesure moins intrusive pour la vie privée a été rejetée, il y a lieu de fournir de bonnes raisons justifiant la non-sélection de cette mesure »[31].

L'exigence de proportionnalité implique également « l'existence de garanties adéquates et suffisantes contre les abus ».[32] Ces garanties doivent inclure l'existence d'une voie de recours effective contre la mesure concernée[33].

Selon la Cour EDH, « la nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (...) »[34]. Outre des « garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs »,[35] le législateur doit également prévoir « l'exercice d'un contrôle indépendant de la justification de la conservation sur la base de critères précis, tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière »[36].

Enfin, l'ingérence dans le droit à la vie privée doit être prévue par une loi « suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu – en s'entourant au besoin de conseils éclairés – de régler sa conduite. Pour que l'on puisse la juger conforme à ces exigences, elle doit fournir une protection adéquate contre l'arbitraire et, en

[25]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 précité, §3.26 (" Plus le problème est grave et/ou plus le dommage ou le préjudice auquel la société peut être exposée estimportant,plus une ingérence peut être justifiée"). Voir également Groupe de travail Article 29 sur la protection des données, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP 217), 9 avril 2014, qui évoque la nécessité de « garanties supplémentaires mises en place par le responsable du traitement afin de prévenir toute incidence injustifiée sur les personnes concernées » : p. 37 ; p.46-47.)

[26]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, 4 décembre 2008, req. n° 30562/04 et 30566/04, § 103, 107.

[27]Cour EDH, 4ème sect., Szabó et Vissy c. Hongrie, 12 janvier 2016, req. n° 37138/14, § 73, § 75-77.

[28]Cour EDH, 5ème sect., D. L. c. Bulgarie, 19 mai 2016, req. n°7472/14, § 105.

[29]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, précité, § 119.

[30]Cour EDH, ch., Crémieux c. France, précité, § 40.

[31]Groupe de travail Article 29 sur la protection des données, Avis 01/2014 précité, §3.26. Voir aussi Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in *The principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, Hart Publishing, 1999, p. 26.

[32]Cour EDH, plen., Klass et autres c. Allemagne, 6 septembre 1978, req. n° 5029/71, § 50.

[33]Cour EDH, 3ème sect., M.N. et autres c. San Marino, 7 juillet 2015, req. n° 28005/12, § 73.

[34]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, précité, § 103.

[35]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, précité, § 103.

[36]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, précité, § 119.

conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes »[37].

2.2.2. La jurisprudence de la CJUE : des exigences équivalentes, en particulier en matière de conservation généralisée de données personnelles

La CDFUE ayant les même sens et portée que la CEDH lorsque les deux instruments juridiques protègent des droits identiques (le droit à la vie privée étant l'un de ces droits)[38], la CJUE a généralement une jurisprudence similaire à celle de la Cour EDH, lorsqu'un cas de même nature lui est soumis. Ainsi, à l'instar de la Cour EDH, elle considère par exemple qu'une mesure limitative de droits, en particulier ceux à la protection de la vie privée et à la protection des données personnelles, ne peut être mise en oeuvre que si elle « est apte à réaliser l'objectif poursuivi »[39] et ne va pas au-delà de ce qui est nécessaire pour atteindre cet objectif[40]. Elle réaffirme que la simple conservation d'une donnée personnelle constitue en soi une ingérence, peu importe, à nouveau, que l'information soit sensible ou que la personne concernée en ait ou non subi un inconvénient[41]. Elle précise que lorsque « d'autres mesures moins attentatoires à la vie privée (sont) envisageables », elles doivent être préférées[42].

En particulier, la CJUE réaffirme que la conservation de données personnelles à des fins de sécurité ne peut pas être de « nature indiscriminée » avant toute suspicion qu'une infraction a été commise par les personnes dont les données sont collectées[43]. Trois arrêts peuvent en particulier être cités en la matière :

Digital Rights Ireland (C-293/12, 8 avril 2014). La CJUE invalide la directive 2006/24/CE sur la conservation des données de communications électroniques. La Cour juge que le législateur a excédé les limites du principe de proportionnalité au regard de plusieurs critères, en particulier les suivants : la directive couvrait l'ensemble des individus sans différenciation ni limitation ; elle ne prévoyait pas de critères objectifs pour définir les infractions graves justifiant l'accès aux données ;

[37]Cour EDH, gr. ch., S. et Marper c. Royaume-Uni, précité, § 95. ; Cour EDH, 3ème sect., G.S.B. c. Suisse, 22 décembre 2015, req. n° 28601/11, § 68.

[38]Article 52,3 de la Charte des droits fondamentaux de l'UE.

[39]CJUE, gr. ch., Digital Rights Ireland et Seitlinger e.a., 8 avril 2014, aff. jointes C-293/12 et C-594/12, § 49. Dans le même sens, Contrôleur européen à la protection des données, Avis sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE), 31 mai 2011, § 41 : « il semble que la Commission se base principalement sur des déclarations des États membres sur leur perception de la conservation des données comme étant un outil nécessaire aux fins de la répression. Ces déclarations, cependant, indiquent plutôt que les États membres concernés sont heureux d'avoir des règles de l'UE sur la conservation des données, mais ne peuvent en soi établir la nécessité de la conservation des données en tant que mesure répressive, encouragée et réglementée par l'UE. Ces déclarations sur la nécessité doivent être corroborées par des éléments de preuve suffisants ».

[40]CJUE, gr. ch., Digital Rights Ireland et Seitlinger e.a., précité, § 52 ; CJUE, 4ème ch., Michael Schwarz c. Stadt Bochum, 17 octobre 2013, aff. C-291/12, § 40. La gravité des impacts doit par ailleurs être justifiée au regard de l'importance de l'objectif visé : CJUE, 4ème ch., Afton Chemical Limited v Secretary of State for Transport, 8 juillet 2010, Aff. C-343/09, §45 ; CJUE, gr. ch., La Quadrature du Net et autres, 6 octobre 2020, aff. jointes C-511/18, C-512/18 et C-520/18, § 131.

[41]CJUE, gr. ch., Digital Rights Ireland et Seitlinger e.a., précité, § 33-34.

[42]Tribunal de la fonction publique (1ère ch.), V. c. Parlement européen, 5 juillet 2011, aff. n° F-46/09, § 103 et 139. Dans le même sens, CJUE, 4ème ch., Afton Chemical Limited v Secretary of State for Transport, précité, §45.

[43]CJUE, Communiqué de presse n° 123/20, Arrêts dans l'affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a, 6 octobre 2020, p.3 : les « obligations de transmission et de conservation généralisée et indifférenciée de [données de trafic] constituent des ingérences particulièrement graves dans les droits fondamentaux garantis par la Charte, sans que le comportement des personnes dont les données sont concernées présente de lien avec l'objectif poursuivi par la réglementation en cause ».

elle ne fixait pas les conditions matérielles et procédurales d'accès ; et elle n'offrait pas de garanties suffisantes contre les risques d'abus et d'accès illicite[44].

Tele2 Sverige / Watson (C-203/15, 21 décembre 2016). La CJUE confirme que les dérogations nationales à l'interdiction de conservation doivent être interprétées strictement et ne peuvent devenir la règle[45].

La Quadrature du Net (C-511/18, 6 octobre 2020). la CJUE réaffirme que le droit de l'UE s'oppose à une conservation généralisée et indifférenciée des données, même pour la lutte contre les infractions graves. La Cour précise que seule une conservation ciblée, fondée sur un lien entre l'objectif de la législation et le comportement des personnes dont les données sont collectées, permettant de penser qu'elles sont impliquées dans la commission de crimes graves, peut être compatible avec la Charte[46].

2.3. Sur la nécessité et la proportionnalité des politiques anti-blanchiment

2.3.1. L'efficacité contestée des politiques anti-blanchiment

Les travaux de Ronald F. Pol (La Trobe University, 2020) établissent que le dispositif mondial anti-blanchiment n'intercepterait que moins de 0,1 % des flux financiers criminels[47]. Europol estime les revenus criminels annuels en Europe à au moins 110 milliards d'euros[48].

Discussion méthodologique. Pol reconnaît que ses données sont insuffisamment validées et que l'écart entre les estimations de revenus criminels et les saisies effectives est difficile à mesurer avec précision. Le GAFI, de son côté, utilise un cadre d'évaluation de l'efficacité fondé sur onze « immediate outcomes », dont Pol souligne qu'ils mesurent des activités et des processus plutôt que des résultats au sens de la science des politiques publiques. L'AMLA, nouvelle autorité européenne installée à Francfort, est censée améliorer la coordination. Le débat n'est pas tranché, mais la charge de la preuve du bénéfice de ces politiques incombe au régulateur, en particulier concernant le bénéfice supplémentaire de la collecte spécifique aux portefeuilles auto-hébergés.

Corroboration institutionnelle. Le 11 mars 2026, la Cour des comptes néerlandaise (Algemene Rekenkamer, institution constitutionnelle indépendante) a publié un audit de l'approche anti-blanchiment dans le secteur bancaire néerlandais. Ses conclusions sont convergentes avec les travaux de Pol[49]. La Cour constate que les contrôles AML ont des « conséquences graves » pour les citoyens et les entreprises, que leurs « avantages restent inconnus », et qu'il existe des « indications de discrimination » : les mosquées et les églises issues des diasporas étant, selon l'audit, soumises à

[44]CJUE, gr. ch., Digital Rights Ireland and Seitlinger and Others, 8 avril 2014, aff. jointes C-293/12 et C-594/12 (invalidation de la directive 2006/24/CE sur la conservation des données). Voir en particulier les § 54-62.

[45]CJUE, gr. ch., Tele2 Sverige et Watson, 21 décembre 2016, aff. jointes C-203/15 et C-698/15. Voir en particulier les § 114-120.

[46]CJUE, gr. ch., La Quadrature du Net et autres, 6 octobre 2020, aff. jointes C-511/18, C-512/18 et C-520/18. Voir en particulier les § 133 et 143-144.

[47]Pol, R.F. (2020). « Anti-money laundering: The world's least effective policy experiment? Together, we can fix it », Policy Design and Practice, 3(1), pp. 73-94. Pol précise que ses données sont « poorly validated » et ses conclusions « cannot be definitive », tout en soulignant un écart considérable entre l'intention politique et les résultats mesurables.

[48]Savona & Riccardi (2015), Project OCP / Transcrime : les marchés illicites dans l'UE génèrent environ 110 Md € par an ; estimation reprise par Europol dans Does crime still pay? (2016).

[49]Voir note 8 supra (Algemene Rekenkamer, 2026) et note 47 supra (Pol, 2020).

des questions plus intrusives sur l'objet et l'origine de leurs transactions que les églises catholiques et protestantes de l'échantillon, y compris pour des transactions ordinaires n'impliquant ni dépôts d'espèces ni transferts internationaux. Les coûts de conformité pour les seules banques néerlandaises atteignent 1,6 milliard d'euros en 2024. Le nombre de transactions inhabituelles signalées est passé de 250 000 en 2020 à 530 000 en 2024, mais la Cour constate que ni les ministères concernés ni la banque centrale (DNB) n'évaluent les résultats de cette approche, et que la FIU néerlandaise ne peut pas déterminer combien de signalements correspondent réellement à du blanchiment.

Ce rapport est d'une pertinence particulière pour la présente note : il émane d'une institution constitutionnelle, il porte sur un État membre de l'UE (les Pays-Bas, qui ont fixé un plafond de 3 000 € pour les paiements en espèces aux commerçants depuis janvier 2026), et il démontre qu'en l'état, la règlementation anti-blanchiment ne répond pas aux exigences de la CEDH et de la CDFUE au regard de la nécessité des limitations de libertés.

Ce rapport remet également en cause la proportionnalité de cette réglementation. La question soulevée par la Cour – les contrôles sont-ils proportionnés à leurs résultats démontrés ? – s'applique a fortiori aux obligations de collecte liées aux portefeuilles auto-hébergés, dont l'efficacité spécifique n'a fait l'objet d'aucune évaluation publiée.

2.3.2. La disproportion manifeste des politiques anti-blanchiment

Alors que la démonstration de l'efficacité des mesures anti-blanchiment n'a pas été faite, les collectes actuelles de données concernent toute personne sans suspicion d'infraction. Cette disproportion manifeste est encore accentuée par les effets contre-productifs de ces mesures qui, en plus d'atteindre le droit à l'auto-détermination des personnes concernées par des mesures de contrôle excessives, mettent ces personnes à risque comme nous le montrons dans notre section suivante relative aux données empiriques, en les privant en outre de tous moyens qui leur permettraient de se protéger de ces risques, incluant les agressions physiques. L'ensemble entre dans la définition des atteintes à la dignité telles que mises en lumière par les cours.

Application au cadre TFR/AMLR. La grille d'analyse livrée par la Cour EDH et la CJUE, en particulier dans son arrêt *Digital Rights Ireland*, soulève notamment un certain nombre de questions que la présente note verse au débat, sans y apporter de réponses définitives : la travel rule et la vérification des portefeuilles auto-hébergés couvrent-elles l'ensemble des utilisateurs sans différenciation ? Quels sont les critères permettant d'assurer que les données collectées ne sont relatives qu'à des personnes susceptibles de préparer une infraction via leurs portefeuilles hébergés ? Les conditions d'accès aux données collectées par les CASP sont-elles encadrées par des critères objectifs et quelles sont les mesures prévues pour garantir l'absence d'arbitraire dans le cadre de ces accès ? Les garanties contre les fuites de données sont-elles suffisantes au regard des risques physiques encourus par les personnes concernées ? Ces questions n'ont pas, à notre connaissance, été publiquement traitées dans les travaux préparatoires du TFR, alors même que les États ont une obligation positive d'assurer la nécessité et la proportionnalité de cette réglementation.

2.3.3. Le standard GAFI : proportionnalité et marge d'adaptation

Le GAFI n'édicte pas un droit directement applicable dans l'ordre juridique de l'Union. Il fixe un standard international d'évaluation, composé de Recommandations, de notes interprétatives et d'un glossaire, que les États et l'Union traduisent ensuite dans leurs instruments juridiques. L'invocation du standard GAFI ne dispense donc pas d'examiner si les mesures adoptées correspondent effectivement à ce que ce standard prescrit.

L'argument administratif selon lequel les obligations de collecte sont dictées par le GAFI et que toute dérogation exposerait l'État à un placement en liste grise appelle un examen factuel. Les Recommandations du GAFI fixent un standard international que chaque pays doit mettre en œuvre « par des mesures adaptées à [ses] circonstances particulières », précisément parce que les pays « ne peuvent pas tous prendre des mesures identiques »[50]. Depuis février 2025, le GAFI a formalisé la proportionnalité comme principe explicite de l'approche fondée sur les risques, en remplaçant le terme « commensurate » par « proportionate » dans la Recommandation 1 et sa Note Interprétative[51]. La Note Interprétative révisée impose désormais aux pays d'autoriser et d'encourager les mesures simplifiées en cas de risque plus faible, et prévoit la possibilité d'exemptions dans des circonstances limitées et justifiées de faible risque évalué (INR.1, § 7-8).

Par ailleurs, le GAFI reconnaît expressément que la lutte AML/CFT et la protection des données personnelles poursuivent toutes deux des objectifs d'intérêt public, au service des droits humains et des libertés fondamentales, et que ces objectifs ne sont pas, par nature, en opposition[52]. Ses standards n'envisagent ni l'exclusion systématique de catégories de clients ni la coupure de classes entières, mais une approche au cas par cas fondée sur le risque[53]. La « liste grise » elle-même correspond à un suivi renforcé pour des déficiences stratégiques, et le GAFI précise qu'il ne demande pas automatiquement l'application de mesures renforcées de vigilance aux juridictions concernées[54].

Implication pour l'analyse. Lorsqu'une autorité nationale ou européenne invoque « le GAFI » pour justifier une collecte systématique sur les portefeuilles auto-hébergés, elle doit démontrer pourquoi cette mesure est proportionnée au risque identifié et pourquoi des moyens moins intrusifs ne suffiraient pas. L'exemple britannique (section 5) montre qu'une mise en œuvre de la travel rule conforme aux standards du GAFI est possible sans collecte systématique. L'argument « sinon on finit en liste grise » est inexact en l'état : la liste grise sanctionne des déficiences stratégiques, pas des adaptations proportionnées des obligations de collecte à un risque évalué comme faible.

[50] GAFI, The FATF Recommendations (version consolidée, mise à jour d'octobre 2025), Introduction, p. 7

[51] GAFI, « FATF updates Standards and consults on guidance to better promote financial inclusion », 25 févr. 2025 ; GAFI, Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures (juin 2025), § 2.3.2, p. 35 ; GAFI, The FATF Recommendations (oct. 2025), Recommandation 1, p. 10, INR.1, §§ 7-8, p. 33, et glossaire, p. 36. En particulier : « proportionate » y est défini comme « a measure or action that appropriately corresponds to the level of identified risk and effectively mitigates the risks » ; les pays doivent « allow and encourage simplified measures » en risque plus faible, avec possibilité d'exemptions en circonstances « limited and justified » d'« assessed low risk ».

[52] GAFI, Stocktake on Data Pooling, Collaborative Analytics and Data Protection (2021), résumé exécutif, p. 5 ; voir aussi GAFI, Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing (2022), résumé exécutif, p. 4.

[53] GAFI, Jurisdictions under Increased Monitoring – 13 February 2026 ; voir aussi GAFI, « FATF clarifies risk-based approach: case-by-case, not wholesale de-risking », 23 oct. 2014.

[54] GAFI, Jurisdictions under Increased Monitoring – 13 February 2026. La « liste grise » renvoie à des juridictions travaillant avec le GAFI pour remédier à des « strategic deficiencies » et soumises à un « increased monitoring » ; le GAFI ajoute explicitement qu'il « does not call for the application of enhanced due diligence measures » à leur égard.

3. Données empiriques

3.1. Part illicite des transactions crypto

Les estimations de la part illicite des flux crypto proviennent d'outils privés d'attribution on-chain. Elles constituent des indications utiles, mais reposent sur des méthodologies propriétaires, partiellement opaques pour le lecteur et non auditables publiquement dans leur détail ; elles doivent donc être lues comme des mesures partielles et révisables, non comme des totaux exhaustifs.

Chainalysis (rapport 2025, données 2024) estimait que les adresses illicites identifiées avaient reçu 40,9 milliards de dollars, soit 0,14 % du volume on-chain attribué. Son rapport 2026 (données 2025) relève au moins 154 milliards de dollars reçus par des adresses illicites, avec une hausse largement tirée par l'activité d'entités sanctionnées ; la part illicite reste inférieure à 1 % du volume attribué. TRM Labs (rapport 2025, données 2024) évaluait l'illicite à 45 milliards de dollars, soit 0,4 % du volume crypto total. Son rapport 2026 (données 2025), fondé sur une méthodologie révisée et un dénominateur différent (le volume on-chain attribué) aboutit à 158 milliards de dollars et 1,2 % de ce volume[55]. Ces séries ne sont pas directement comparables entre elles, mais elles convergent vers un même ordre de grandeur : l'activité illicite identifiée reste minoritaire.

Limites et portée. Ces estimations sont des bornes basses, révisées à la hausse à mesure que de nouvelles adresses illicites sont identifiées. Les crimes non natifs crypto, par exemple un narcotrafic réglé en crypto-actifs, sont largement indiscernables on-chain et donc exclus de ces mesures. Les catégories, les dénominateurs et les modèles de classification varient selon les fournisseurs. L'argument de la présente note ne repose donc pas sur la précision d'un taux unique, mais sur un ordre de grandeur convergent : même en tenant compte de révisions significatives et d'une opacité méthodologique partielle, l'activité illicite identifiée n'approche pas un niveau majoritaire des flux.

Implication pour l'analyse de proportionnalité. Si l'ordre de grandeur demeure celui d'un phénomène minoritaire, une obligation de collecte systématique couvrant l'ensemble des utilisateurs au-delà de 1 000 € n'est pas acceptable sans critères supplémentaires permettant d'établir un lien entre les personnes concernées par la collecte et une suspicion d'infraction grave, que le critère de limitation intervienne dans le temps, l'espace ou sur d'autres critères objectifs, suivant la grille de lecture fournie par les cours de justice. Le bénéfice de la mesure dans la lutte contre le blanchiment doit par ailleurs être démontré.

3.2. Incidents de cybersécurité des institutions européennes

Note méthodologique : pour l'incident de mars 2026, le communiqué officiel de la Commission confirme une cyberattaque sur l'infrastructure cloud Europa.eu et indique que des données ont pu être dérobées[56]. Les allégations de ShinyHunters ne sont pas confirmées à ce stade.

[55] Chainalysis, 2025 Crypto Crime Report, janvier 2025 (données 2024) ; 2026 Crypto Crime Report, mars 2026 (données 2025). TRM Labs, 2025 Crypto Crime Report, février 2025 (données 2024) ; 2026 Crypto Crime Report, janvier 2026 (données 2025).

[56] Commission européenne, communiqué du 27 mars 2026. La Commission précise que ses systèmes internes n'ont pas été affectés. Les allégations de ShinyHunters (350 Go) sont rapportées par BleepingComputer, Cybernews, Infosecurity Magazine et n'ont pas été officiellement confirmées.

Date	Institution	Fait confirmé	Allégations non confirmées
Mars 2026	Commission européenne (Europa.eu)	Cyberattaque ; données possiblement dérobées ; systèmes internes non affectés	ShinyHunters : 350 Go (mail, BDD, DKIM, SSO)
Janv. 2026	Com. européenne (MDM)	Violation plateforme appareils mobiles	Noms, téléphones du personnel
2024	Parlement européen	Violation découverte (prép. élections)	Périmètre non précisé
2020	Institutions UE	Données de fonctionnaires UE exposées en ligne (chiffre de 1 200 rapporté par la presse, source institutionnelle non identifiée)	—
2014	BCE	Violation BDD, tentative rançon	20 000 emails, contacts

En 2025, 443 violations de données étaient rapportées quotidiennement en Europe (+22 %)[57]. Le montant cumulé des amendes RGPD dépasse 7,1 milliards d'euros depuis 2018.

3.3. Le cas Ledger : démonstration empirique de l'irréversibilité

La violation de la base de données e-commerce de Ledger en juin 2020 constitue le cas d'étude le plus documenté des conséquences spécifiques d'une fuite de données crypto-financières.

Les faits. Une clé API d'un outil marketing tiers, mal configurée, a permis l'accès à la base de données e-commerce de Ledger en juin 2020. Ledger a initialement annoncé l'exposition d'environ 1 million d'adresses e-mail et de 9 532 enregistrements détaillés. En décembre 2020, la publication de la base sur le forum RaidForums a révélé un périmètre nettement plus large : environ 272 000 enregistrements détaillés (noms, adresses postales, téléphones). Un incident distinct, impliquant des agents du prestataire e-commerce Shopify, a été signalé la même semaine. La CNIL a condamné Ledger à une amende de 750 000 € par décision du 10 octobre 2024, pour défaut de sécurisation et durée excessive de conservation des données[58].

La chaîne d'exploitation. La fuite Ledger ne portait pas sur des clés privées ni sur des adresses de portefeuilles. Elle portait sur des données « non sensibles » au sens classique : noms et adresses postales de clients ayant acheté un portefeuille matériel. Pourtant, cette information « méta » est devenue un outil de ciblage précis : une adresse de livraison d'un portefeuille matériel est un signal fort de détention de crypto-actifs. L'attaquant sait où vit un détenteur probable. Si cette identité peut être rattachée à des adresses on-chain (via des données KYC d'une plateforme d'échange, une adresse de donation publique, ou toute autre trace liant un nom à une adresse blockchain), l'attaquant peut alors associer un patrimoine estimé à une adresse physique. Ce croisement entre données d'identité et blockchain publique est le mécanisme central du risque analysé dans la présente note.

[57] DLA Piper, GDPR Fines and Data Breach Survey: January 2026, 21 janv. 2026 : le total agrégé des amendes RGPD signalées depuis l'entrée en application du règlement, le 25 mai 2018, jusqu'au 10 janv. 2026, atteint 7,1 milliards d'euros. V. aussi CMS, GDPR Enforcement Tracker, statistiques cumulées des amendes, base de données en ligne (non exhaustive, toutes les amendes n'étant pas rendues publiques).

[58] V. supra, note 4

L'irréversibilité démontrée. Cinq ans après la fuite, les données Ledger continuent d'alimenter des campagnes de phishing (y compris des lettres physiques envoyées aux adresses postales en 2025), des emails d'extorsion menaçant d'intrusion dans le domicile, et des tentatives de vols sous contrainte. Contrairement à une fuite bancaire où les cartes sont révoquées et les comptes clos, l'adresse postale ne peut pas être « révoquée », et l'information que son occupant détient des crypto-actifs ne peut pas être « désassociée ».

Transposition au cadre AMLR/TFR. Les données que l'AMLR et le TFR imposent aux CASP de collecter (identité civile associée à une adresse de portefeuille et un historique de transactions) sont structurellement plus riches que les données Ledger (qui ne contenaient ni adresses de portefeuilles ni historiques). En cas de fuite d'une base CASP, l'attaquant dispose directement de l'association identité/adresse crypto/montants, sans avoir besoin d'inférer quoi que ce soit. Le préjudice potentiel est donc supérieur à celui documenté dans le cas Ledger et serait sans aucun doute qualifié d'intolérable par la Cour EDH et la CJUE.

4. Le cas français : fuites de données et agressions physiques

4.1. Panorama factuel

La France connaît depuis janvier 2025 une vague sans précédent des agressions physiques visant des détenteurs de crypto-actifs. Selon CertiK, la France a enregistré 19 incidents physiques vérifiés sur 72 recensés dans le monde en 2025, soit 26,4 % des cas mondiaux pour moins de 1 % de la population mondiale. Les données disponibles pour 2026 suggèrent une aggravation : selon le tracker public de Jameson Lopp (méthodologie distincte de CertiK), la France concentrait deux tiers des 24 attaques recensées depuis le 1er janvier 2026[59].

Le profil des agressions a évolué. Les cas médiatisés incluent des enlèvements avec mutilations et un ciblage croissant de l'entourage familial des détenteurs, utilisé comme levier de pression.

4.2. Le lien documenté entre fuites de données et ciblage

L'affaire Ghalia C. En juillet 2025, une agente des impôts a été mise en examen à Bobigny pour avoir utilisé ses accès fiscaux pour rechercher diverses cibles, dont des investisseurs en cryptomonnaie, et transmettre des informations à un réseau criminel[60]. Cette affaire démontre que la centralisation de données fiscales crée un risque d'exploitation interne, même en l'absence de cyberattaque.

Les fuites de plateformes privées. Des fuites de données de CASP et de prestataires fiscaux crypto (notamment Waltio) font l'objet d'enquêtes et nourrissent des soupçons sérieux quant à leur exploitation dans des vols suivis d'agressions physiques[61]. Cybermalveillance.gouv.fr souligne

[59] Lopp, J., "Known Physical Bitcoin Attacks", dépôt GitHub (github.com/jlopp/physical-bitcoin-attacks). Liste publique non exhaustive ; l'auteur précise que de nombreuses attaques ne sont pas publiquement rapportées. Consulté le 31 mars 2026.

[60] Le Parisien, Jérémie Pham-Lê et Jean-Michel Décugis, « Une agente des impôts soupçonnée d'informer le crime organisé », 3 juill. 2025 (parquet de Bobigny : mise en examen notamment pour « participation à une association de malfaiteurs », « complicité de violences aggravées » et « complicité de menaces », après des recherches illégitimes dans la base fiscale) ; Julien Constant, « L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaie pour un mystérieux commanditaire », 6 janv. 2026 (recherches relevées sur des investisseurs en cryptomonnaie et autres cibles).

[61] Cybermalveillance.gouv.fr, "Violation de données personnelles dans le secteur des crypto-actifs", 22 janv. 2026 (mis à jour le 3 févr. 2026) : enquête préliminaire en cours concernant Waltio, diligentée par le Parquet de Paris ; les investigations doivent déterminer la nature précise des données dérobées et identifier les clients concernés.

d'ailleurs que, dans les cas les plus graves, ce type de fuite peut conduire à des menaces et à des agressions physiques visant les victimes ou leur entourage. Dans les affaires médiatisées, les assaillants disposaient d'informations d'une précision (adresses postales exactes, estimation des montants détenus) qui ne relèvent pas de l'observation de réseaux sociaux mais supposent l'accès à des bases de données consolidées.

4.3. Au-delà des crypto-actifs : la centralisation comme vecteur de risque systémique

Le risque analysé dans la présente note n'est pas spécifique aux crypto-actifs. Il touche toute base de données centralisée associant identités civiles et actifs de valeur localisés physiquement.

Le cas du SIA (mars 2026). Le ministère de l'Intérieur a confirmé, la même semaine que la violation d'Europa.eu, la compromission d'un compte du Système d'information sur les armes (SIA)[62]. Un hacker revendique la vente de données liées à 62 511 armes et leurs propriétaires. La logique est structurellement identique : l'État impose la centralisation de données sensibles dans un registre (à des fins de sécurité publique), cette centralisation crée une cible de haute valeur, et lorsque la base est compromise, le préjudice va au-delà de l'atteinte à la vie privée : il permet le ciblage physique de propriétaires d'actifs identifiés et localisés.

Ce parallèle montre que la question posée par la présente note est une question d'intérêt général sur l'architecture des systèmes de collecte, et non une question sectorielle liée aux seuls crypto-actifs.

5. Alternatives réglementaires : ce que montre, et ne montre pas, le cas britannique

Le cas britannique n'est pas présenté ici comme un modèle normatif. Il est mobilisé uniquement pour montrer que la combinaison retenue par l'Union (logique prescriptive et seuil uniforme de 1 000 € pour l'appréciation du contrôle d'une adresse auto-hébergée) n'était pas la seule architecture réglementaire concevable. Le HM Treasury britannique a explicitement déclaré que les transactions avec des portefeuilles auto-hébergés ne devaient pas être automatiquement considérées comme présentant un risque plus élevé[63]. Le cadre britannique repose davantage sur une appréciation du risque au niveau de l'entreprise (firm-level assessment) que sur un seuil uniforme. Cette différence a une valeur démonstrative institutionnelle : le design européen n'était pas inévitable.

Portée et limites de la comparaison. Le Royaume-Uni n'est plus membre de l'UE et son marché diffère par sa taille et sa structure. Les données sectorielles disponibles sur les taux de conformité respectifs sont d'origine industrielle et ne permettent pas de conclusions robustes. En conséquence, cette comparaison ne permet ni d'établir la supériorité du régime britannique, ni de conclure à sa conformité au regard des principes de nécessité et de proportionnalité et des objections de principe soulevées par la présente note quant à la collecte centralisée, à la conservation des données et à l'irréversibilité du préjudice en cas de fuite.

[62] Ministère de l'Intérieur, confirmation au Parisien le 30 mars 2026 : compromission d'un compte professionnel ayant accès au Système d'information sur les armes (SIA). Le ministère précise que le SIA lui-même n'a pas été atteint.

[63] UK HM Treasury, Response to the Consultation: Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, juin 2022, paras. 6.21-6.22, pp. 29-30

6. Analyse : le test de proportionnalité revisité

6.1. Le bénéfice attendu à la lumière des données

L'objectif du cadre AMLR/TFR est légitime. La question n'est pas de contester cet objectif, mais d'évaluer si les moyens choisis sont adaptés et proportionnés. Deux éléments empiriques méritent examen.

Premièrement, si la part illicite des transactions crypto, malgré l'opacité partielle des outils de mesure, demeure d'un ordre de grandeur minoritaire selon les principaux fournisseurs de données on-chain, et que la blockchain offre déjà une traçabilité native, la question du bénéfice supplémentaire apporté par l'identification systématique par rapport à la traçabilité native de la blockchain se pose avec acuité.

Deuxièmement, l'asymétrie des seuils entre instruments mérite documentation. Le seuil de CDD pour les CASP est de 1 000 €; le seuil général est de 10 000 €. Le plafond cash UE sera de 10 000 € à compter de juillet 2027[64], avec des seuils nationaux pouvant être plus bas[65]. Cette asymétrie peut refléter des profils de risque différents, mais devrait être étayée par des données empiriques comparant les taux d'utilisation illicite des différents instruments.

À cet égard, le superviseur français documente lui-même, au sein de l'infrastructure de paiement classique, des concentrations de risque sur des configurations techniques précises. Le rapport ACPR/Tracfin d'avril 2026 sur les IBAN virtuels distingue des usages majoritairement légitimes et des cas d'usage à risque élevé, notamment lorsque le code pays de l'IBAN est dissocié du lieu de tenue du compte. Dans ce sous-ensemble limité, les rares établissements concernés représentaient environ 20 % de la valeur des demandes de retours de virement pour motif de fraude en France, pour moins de 0,5 % des paiements reçus. Ce constat ne suffit ni à conclure à une hiérarchie générale entre instruments ni à justifier un alignement par le haut des obligations de collecte. Il montre en revanche que des concentrations de risque très marquées existent aussi dans l'infrastructure bancaire classique et que l'asymétrie des seuils ne peut être tenue pour acquise sans démonstration empirique comparative[66].

Troisièmement, le cadre TFR/AMLR va au-delà de ce que le GAFI impose. Le GAFI fixe un standard fondé sur le risque, prévoyant expressément des mesures simplifiées en cas de risque plus faible et des exemptions en cas de risque faible évalué. Or, la collecte systématique sur les portefeuilles auto-hébergés au-delà de 1 000 € n'est pas assortie d'une évaluation publiée du gain qu'elle apporte par rapport aux outils d'analyse existants ; les transactions sur les blockchains publiques étant, par construction, consultables par quiconque. L'écart entre le standard GAFI (proportionnalité au risque identifié) et l'obligation européenne (collecte uniforme au-delà d'un seuil bas) présente ainsi les caractéristiques d'une surtransposition, dont la justification empirique reste à démontrer.

[64] AMLR, art. 80 : plafond UE de 10 000 € pour paiements en espèces (juillet 2027). Les États membres peuvent fixer des seuils inférieurs.

[65] France : plafond espèces 1 000 € (art. L.112-6 CMF). Pays-Bas : 3 000 € (2025).

[66] ACPR / Tracfin, Panorama et analyse des services d'IBAN virtuels offerts en France, sous l'angle de la lutte contre le blanchiment des capitaux et le financement du terrorisme, avril 2026, synthèse p. 3 ; section II, cas n° 5, p. 16-18 et 23-24.

6.2. Le transfert de l'évaluation des risques aux acteurs privés et l'incitation structurelle à la surconformité

Le débat de proportionnalité ne porte pas seulement sur ce que le texte exige en droit, mais aussi sur l'architecture d'incitations qu'il crée. Lorsqu'un régime impose aux CASP de prendre des « mesures adéquates » pour apprécier si une adresse auto-hébergée est détenue ou contrôlée par leur client, tout en leur imposant des politiques, procédures et contrôles internes spécifiques, il leur transfère une part substantielle de l'évaluation opérationnelle du risque LBC/FT.

En pratique, l'arbitrage est déplacé. En effet, la fonction d'évaluation n'est plus exercée seulement ex post par le superviseur ; elle est déplacée vers des acteurs privés qui doivent arbitrer eux-mêmes, au quotidien, entre risque prudentiel, coût de conformité et continuité de la relation client.

Or les incitations sont asymétriques. Pour un CASP, le coût d'une sous-évaluation du risque est potentiellement élevé : grief du superviseur, sanction, remise en cause des dispositifs internes, risque réputationnel. À l'inverse, le coût d'une sur-évaluation est diffus et principalement supporté par l'utilisateur : demandes documentaires supplémentaires, délais, refus de service, conservation élargie de données ou exposition accrue au risque de fuite. En l'absence de critères objectivés et d'un espace de sécurité juridique permettant de ne pas surcollecter, le comportement rationnel de l'acteur privé n'est pas la minimisation, mais la prudence défensive.

Cette logique se manifeste de trois manières. Premièrement, par le de-risking : plutôt que d'opérer une évaluation granulaire du risque, l'acteur privé peut être incité à restreindre certaines relations ou certaines opérations jugées plus exposées. Deuxièmement, par la sur-déclaration : lorsqu'un défaut de signalement paraît plus coûteux qu'un excès de signalement, le système tend à produire davantage d'alertes que de renseignement utile. Troisièmement, par la surcollecte : le CASP est incité à demander, documenter et conserver plus d'informations qu'il n'est strictement nécessaire d'en traiter, parce que le coût d'un déficit documentaire est internalisé par lui, tandis que le coût du risque de fuite est largement externalisé sur l'utilisateur.

Cette dynamique a une conséquence institutionnelle importante : l'État ne collecte pas nécessairement lui-même toutes les données, mais il construit un régime d'incitations qui pousse les acteurs privés à le faire de manière préventive. La responsabilité publique devient alors moins visible, tandis que les critères effectivement appliqués deviennent fragmentés, opaques, variables d'un établissement à l'autre et difficiles à contester. Les faux positifs, les restrictions d'accès et certaines formes de discrimination peuvent ainsi être compris non comme des accidents extérieurs au système, mais comme des effets prévisibles d'un cadre où la sous-conformité est beaucoup plus sévèrement sanctionnée que la surconformité.

Cette dynamique entre en tension structurelle avec le principe de proportionnalité, incluant la minimisation. Si l'architecture réglementaire incite structurellement à collecter « plus au cas où », la tension avec la CEDH, la CDFUE et le RGPD ne résulte plus seulement d'incidents ponctuels ou de mauvaises pratiques individuelles ; elle devient en partie une propriété prévisible du dispositif, faute pour ce dernier de prévoir des garanties suffisantes contre l'arbitraire. Le problème de proportionnalité ne se réduit donc pas à la question : « que demandent exactement les textes ? » Il inclut aussi la question : « qu'incitent-ils rationnellement les acteurs privés à faire ? »

Les constats de la Cour des comptes néerlandaise peuvent être lus à cette lumière : conséquences graves pour les citoyens et les entreprises, avantages inconnus, indications de discrimination et hausse massive des signalements (de 250 000 en 2020 à 530 000 en 2024) sans mesure claire de leur utilité réelle[67]. Sans établir à elle seule une quantification exhaustive de la surcollecte ou du de-risking à l'échelle de l'Union, la présente analyse montre que ces effets sont structurellement prévisibles au regard de l'architecture des incitations.

6.3. Le risque à la lumière du cas Ledger et des agressions françaises

L'irréversibilité du préjudice n'est plus un argument théorique. Le cas Ledger démontre empiriquement qu'une fuite de données associant identités et détention de crypto-actifs produit des conséquences durables et non remédiables. Le cas français démontre que ces conséquences incluent des atteintes à l'intégrité physique, et pas seulement à la vie privée. L'affaire Ghalia C. démontre que la centralisation crée un risque d'exploitation interne, même en l'absence de cyberattaque. Plus une base est riche en données d'identité, d'adresses de portefeuille et d'historique transactionnel, plus elle constitue une cible de valeur pour un attaquant ou un initié malveillant.

Au regard de l'article 25 du RGPD (protection dès la conception), si la protection adéquate ne peut pas être garantie, et les incidents répétés suggèrent que cette garantie est fragile, le principe de minimisation commande de reconsidérer le volume de données collectées. Le risque documenté par Ledger n'est donc pas seulement un argument contre la centralisation de données ; il est aussi un argument contre tout cadre qui incite les acteurs privés à enrichir ces bases au-delà du strict nécessaire pour atteindre l'objectif de la réglementation.

À cet égard, l'article 35 du RGPD impose une analyse d'impact relative à la protection des données (AIPD) lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes. Cette analyse, qui inclut une évaluation des risques pour les libertés et des mesures envisagées pour y faire face, constitue une garantie structurelle de nécessité et de proportionnalité, en amont de la mise en œuvre du traitement. Elle est a fortiori attendue pour un dispositif de collecte systématique associant identité civile, adresse cryptographique et historique transactionnel, dont le cas Ledger et les affaires françaises documentent le risque pour l'intégrité physique des personnes concernées. À notre connaissance, aucune AIPD publique consolidée ne couvre, à l'échelle de l'Union, le périmètre CASP et l'interaction avec les portefeuilles auto-hébergés tel qu'il résulte de l'AMLR et du TFR.

[67] Algemene Rekenkamer (Cour des comptes néerlandaise), « Anti-money laundering checks: serious consequences for citizens, unknown benefits », 11 mars 2026 (coûts de conformité estimés à 1,6 Md€ pour les banques néerlandaises en 2024 ; signalements de transactions inhabituelles passés de 250 000 en 2020 à 530 000 en 2024 ; absence d'évaluation claire de l'utilité réelle de ces signalements).

6.4. Mise en regard du cadre TFR/AMLR avec les exigences de la CJUE dans son arrêt Digital Rights Ireland

Critère CJUE	Dir. 2006/24 (invalidée)	Cadre TFR/AMLR (portefeuilles auto-hébergés)	Observation
Couverture	Ensemble des individus, sans différenciation ni lien avec une infraction	Toute transaction >1 000 € avec portefeuille auto-hébergé, sans soupçon individualisé	À examiner : la couverture repose-t-elle sur un critère objectif de risque ?
Critères d'accès	Aucun critère objectif pour définir les infractions graves	Conditions d'accès aux données détenues par les CASP : cadre national variable	À documenter : le cadre d'accès est-il harmonisé au niveau UE ?
Garanties contre les abus	Insuffisantes selon la CJUE	Obligations RGPD génériques ; pas d'analyse d'impact préalable (art. 35 RGPD) publiée sur le périmètre CASP / portefeuilles auto-hébergés	À évaluer : absence d'AIPD publiée ; garantie structurelle manquante.
Durée de conservation	6 à 24 mois (critiqué)	Durée fixée par l'AMLR : 5 ans après la fin de la relation client	À noter : durée plus longue que la directive invalidée

Ce tableau fait apparaître plusieurs points de tension entre le cadre TFR/AMLR et la jurisprudence. Les contextes juridiques et factuels diffèrent en ce que la directive 2006/24 portait sur les communications électroniques et non sur les transactions financières. Ceci étant dit, les données financières sont couvertes par la protection offerte à la vie privée, selon la Cour EDH. La CJUE ne s'est pas prononcée sur la question car elle n'en a pas eu l'occasion. En tout état de cause, les informations bancaires sont objectivement aussi sensibles, si ce n'est plus, que des données de trafic et de localisation : elles révèlent les choix et habitudes de vie d'une personne, souvent sa localisation, outre le fait que leur connaissance par des tiers non habilités dans un objectif strictement légitime et respecté peut mettre à risque l'intégrité physique et psychique de cette personne. Tenant l'ensemble de ces éléments et le fait que la réglementation actuelle ne permet pas aux personnes concernées de se protéger des atteintes physiques que la réglementation induit elle-même, cette perte de contrôle injustifiée équivalant à une atteinte à la dignité selon les cours, il est difficilement envisageable que la CJUE ne suive pas la jurisprudence de la Cour EDH sur cette question.

6.5. Ce que le standard GAFI exige, et ce qu'il n'exige pas

Pris ensemble, les textes primaires du GAFI conduisent à une conclusion plus étroite que celle souvent avancée dans le débat public. Ils imposent une approche fondée sur les risques, autorisent des adaptations nationales, renforcent les mesures simplifiées en situation de risque moindre et n'assimilent pas la « liste grise » à une sanction automatique attachée à toute divergence d'interprétation.

La vraie question, pour le cas des portefeuilles auto-hébergés, n'est donc pas de savoir si l'Union peut invoquer le GAFI, mais si elle démontre pourquoi une collecte uniforme au-delà de 1 000 euros serait nécessaire et proportionnée, et pourquoi une approche plus ciblée — à l'image du précédent britannique — ne suffirait pas. Tant que cette démonstration n'est pas publiée, l'argument d'inévitabilité demeure incomplet.

7. Limites et objections

Objection 1 : les violations de données ne justifient pas l'abandon de la collecte. Le principe de minimisation n'exige pas l'absence de collecte mais sa proportionnalité. La spécificité irréversible des données crypto-financières appelle un examen de proportionnalité plus exigeant, pas une prohibition.

Objection 2 : les travaux de PoI ne sont pas transposables à l'AMLR. Point méthodologique valide, discuté en section 2.4. L'AMLR pourrait améliorer l'efficacité. Mais en l'absence d'étude d'impact publiée sur l'efficacité de la collecte relative aux portefeuilles auto-hébergés, la question de son bénéfice reste ouverte.

Objection 3 : l'incident Europa.eu ne concerne pas les données CASP. Exact. L'argument n'est pas de causalité directe mais de démonstration du niveau général de risque. Si les institutions qui définissent les normes de cybersécurité ne protègent pas leurs propres systèmes, les CASP de taille plus modeste font face au même défi.

Objection 4 : l'asymétrie des seuils reflète des risques différents. Position défendable, mais qui devrait être étayée par des données comparatives. Le rapport art. 37(2) TFR est la fenêtre légitime pour cette évaluation.

Objection 5 : les données Chainalysis sous-estiment l'activité illicite. C'est exact en un sens : Chainalysis reconnaît que ses estimations sont des bornes basses, révisées à la hausse en moyenne de 25 % par an, et les crimes non-natifs crypto sont exclus. Mais cette limite ne suffit pas à invalider l'argument. D'une part, d'autres fournisseurs privés d'analyse on-chain, notamment TRM Labs et, sur séries antérieures, Elliptic, aboutissent à des ordres de grandeur comparables, malgré des dénominateurs et des classifications différents. D'autre part, l'argument de la note ne repose pas sur la précision d'une estimation ponctuelle, mais sur un ordre de grandeur convergent : même en tenant compte de l'opacité partielle des méthodologies utilisées, l'activité illicite identifiée demeure minoritaire au regard du volume total. Enfin, les cours de justice sont formelles sur le fait que la responsabilité de la démonstration de l'efficacité de la mesure repose sur l'Etat.

Objection 6 : le cas britannique fournit déjà une solution équilibrée. Il fournit un contre-exemple utile pour montrer que le seuil uniforme de 1 000 € et l'automaticité présumée du risque n'étaient pas inévitables ; il ne suffit pas, à lui seul, à lever les objections de principe relatives à la minimisation des données, à la centralisation des informations et à l'irréversibilité du préjudice en cas de fuite.

Objection 7 : la surconformité est un problème de mise en œuvre, pas de conception. Le superviseur pourrait corriger la surconformité par ses pratiques de contrôle. C'est théoriquement possible, mais en l'absence de zone de sécurité juridique explicite pour les CASP qui choisissent de ne pas surcollecter, et tant que seule la sous-conformité fait l'objet de sanctions, l'asymétrie d'incitations reste structurelle. L'AMLA pourrait faire évoluer cette situation ; ses orientations de supervision seront à évaluer. Plus loin, c'est précisément pour éviter cet arbitraire que les cours de justice imposent que la loi soit claire et prévisible, notamment dans les garanties de proportionnalité à mettre en place.

Limite probatoire. Pour l'incident de mars 2026, la note s'appuie sur le communiqué officiel et des sources journalistiques. Pour le SIA, le ministère de l'Intérieur a confirmé la compromission d'un

compte mais les allégations du hacker (62 511 armes) ne sont pas vérifiées. L'analyse devra être révisée.

8. Conclusions

La présente note a versé au débat huit éléments empiriques et analytiques :

- La part illicite des transactions crypto est estimée comme minoritaire par plusieurs fournisseurs d'analyse on-chain, malgré des méthodologies propriétaires et des dénominateurs différents (Chainalysis : moins de 1 % du volume attribué ; TRM Labs : 1,2 % du volume on-chain attribué pour 2025), ce qui conduit à raisonner en ordre de grandeur plutôt qu'à partir d'un chiffre unique et soulève la question du bénéfice d'une collecte couvrant l'ensemble des utilisateurs ; sans bénéfice avéré, la collecte de ces données soulève un doute sérieux quant à sa compatibilité avec la CEDH et à la CDFUE.
- Les données crypto-financières centralisées présentent un risque spécifique d'irréversibilité en cas de fuite, empiriquement démontré sur cinq ans par le cas Ledger. Ce risque d'atteinte aux personnes serait certainement considéré comme intolérable par la Cour EDH et la CJUE, à tout le moins disproportionné eu égard aux faibles bénéfices de la mesure qui ont été pour l'heure démontrés.
- Le lien entre centralisation de données et ciblage physique est documenté en France (affaire Ghalia C. : exploitation interne de données fiscales ; cas Waltio : enquêtes en cours), dans un contexte où le pays concentre un quart des agressions mondiales (CertiK, 19 cas sur 72) ;
- La jurisprudence de la Cour EDH et de la CJUE, en premier lieu les arrêts de cette dernière *Digital Rights Ireland*, Tele2* et La Quadrature du Net**, fournit une grille d'analyse exigeante applicable, par analogie, au cadre TFR/AMLR ;
- Le cas britannique montre que le seuil uniforme de 1 000 euros et la logique prescriptive retenus par l'UE n'étaient pas des choix réglementaires inévitables ; cette comparaison ne permet toutefois ni d'ériger le Royaume-Uni en modèle, ni de lever à elle seule les objections de principe soulevées par la présente note ;
- La Cour des comptes néerlandaise (Algemene Rekenkamer, mars 2026) conclut que les contrôles anti-blanchiment ont des conséquences graves pour les citoyens, que leurs avantages restent inconnus, et qu'il existe des indications de discrimination, corroborant au niveau institutionnel le diagnostic académique de Pol sur l'inefficacité du dispositif.
- Le GAFI formalise depuis 2025 la proportionnalité comme principe explicite, prévoit des mesures simplifiées et des exemptions en risque faible, et ne prescrit ni collecte uniforme ni exclusion systématique de catégories de clients ; le cadre européen peut ainsi être regardé comme allant au-delà du standard GAFI sur les portefeuilles auto-hébergés ;
- Le transfert de l'évaluation des risques aux acteurs privés, dans un cadre où la sous-conformité est sévèrement sanctionnée mais la surconformité ne l'est pas, crée une incitation structurelle à la surcollecte, à l'inflation des signalements et à des restrictions d'accès défensives. Il est de fait difficilement compatible avec les exigences posées par la CEDH et à la CDFUE, lesquelles exigent que la minimisation soit en premier lieu organisée par le législateur par l'intermédiaire de garanties claires et prévisibles contre l'arbitraire.

Le point n'est pas d'opposer les libertés fondamentales au GAFI. Il est de rappeler que les mesures européennes doivent aussi satisfaire au test que le GAFI pose lui-même : approche fondée sur les risques, proportionnalité, mesures simplifiées en risque moindre et refus de l'exclusion généralisée de catégories de clients.

Le rapport de la Commission prévu à l'article 37(2) du TFR, dont l'échéance est fixée au 1er juillet 2026, constitue la fenêtre réglementaire pertinente pour intégrer ces éléments. À notre sens, il devrait évaluer non seulement les risques de blanchiment liés aux portefeuilles auto-hébergés, mais aussi la nécessité, la portée et les risques propres de la collecte centralisée elle-même, les architectures de conformité permettant de réduire au minimum le volume, la sensibilité et la durée de conservation des données, ainsi que les effets de la délégation de l'évaluation du risque aux acteurs privés, dès lors que cette délégation peut conduire, par prudence défensive, à une surcollecte systémique.

L'actualité de cette analyse est renforcée par un développement législatif français récent. *L'Assemblée nationale a adopté le 7 avril 2026, en première lecture, un amendement imposant la déclaration annuelle des portefeuilles auto-hébergés au-delà de 5 000 euros. Cette obligation créerait, sur les serveurs de l'administration fiscale, une base de données centralisée associant identités civiles et valeur des portefeuilles détenus en propre, exactement le type de centralisation dont la présente note documente les risques. Le texte doit désormais faire l'objet d'une commission mixte paritaire. Selon le dossier législatif du Sénat, cette CMP doit se réunir le 28 avril 2026 ; la lecture de ses conclusions à l'Assemblée nationale était ensuite inscrite à l'ordre du jour du 5 mai 2026, sous réserve de leur dépôt.*

Contribution externe

Contribution et relecture externes sur la discussion juridique : Estelle De Marco, docteure en droit, experte auprès d'Expertise France (programme OCWAR-C) et précédemment auprès du Conseil de l'Europe en cybercriminalité et droits fondamentaux.

Bastien Desteuque, directeur général de l'INBi

L'Institut National de Bitcoin (INBi) est une association loi 1901. Ses travaux portent sur les systèmes monétaires, l'énergie et les libertés. L'INBi agit de manière indépendante et apartisane.