NOTE DE RECHERCHE

*Libertés et souveraineté numérique*

# Contrôler sans ficher : ce qui se joue pour les adresses auto-hébergées

*Ce qui s'applique déjà, ce qui s'écrira d'ici 2027, et les bornes qui éviteraient la surcollecte par défaut.*

Juillet 2026

INBi – www.inbi.fr

Le 10 juillet 2026, l'Autorité européenne de lutte contre le blanchiment (AMLA) doit soumettre à la Commission une première série de projets de normes techniques de réglementation (RTS) du nouveau cadre européen anti-blanchiment, dont le RTS de vigilance client prévu à l'article 28(1) du règlement (UE) 2024/1624 (AMLR).

Qu'est-ce que cela change, concrètement, pour les adresses auto-hébergées ? Pour y répondre, il faut tenir compte de trois textes qui ne vivent pas au même rythme. Le règlement sur les transferts de fonds et de certains crypto-actifs (TFR, règlement (UE) 2023/1113) s'applique déjà, depuis fin 2024. Le règlement anti-blanchiment lui-même ne s'appliquera qu'au 10 juillet 2027, et c'est lui qui porte, à son article 40, le régime dédié aux adresses auto-hébergées. Entre les deux, le RTS de vigilance client transmis ce 10 juillet fixe un socle commun à tous les assujettis, qui ne dit rien de spécifique sur ces adresses.

Les adresses auto-hébergées n'échappent donc pas au cadre anti-blanchiment. Mais la question est de savoir si l'approche par les risques restera une approche graduée, ou si elle sera transformée, par prudence opérationnelle, en collecte maximale par défaut.

## 1. Ce qui est déjà applicable : le TFR et la Travel Rule

Depuis le 30 décembre 2024, les prestataires de services sur crypto-actifs (CASP) appliquent le TFR. Pour les transferts impliquant une adresse auto-hébergée, le texte impose la collecte et la conservation d'informations permettant d'identifier le transfert et, au-delà de 1 000 euros, l'appréciation de la détention ou du contrôle de l'adresse par le client concerné ; côté envoi comme côté réception (articles 14(5) et 16(2) du TFR).

Les orientations de l'Autorité bancaire européenne (EBA/GL/2024/11, applicables depuis la même date) en précisent déjà l'application. Elles citent plusieurs méthodes de vérification (envoi d'un montant prédéfini, signature d'un message au moyen de la clé correspondant à l'adresse, ou tout autre moyen technique fiable). Elles ajoutent un point structurant : le prestataire qui a établi la détention ou le contrôle de l'adresse par son client peut le documenter dans ses systèmes, jusqu'à l'inscription sur liste blanche ; avec retrait si le risque ou le contrôle de l'adresse change.

Ce constat n'est pas un satisfecit : c'est le point de référence. La gradation par le risque (vérifier le contrôle, documenter, réexaminer sur indice) est déjà le principe du droit applicable. Les textes d'application à venir devraient préciser cette gradation, non la remplacer par une règle uniforme de collecte.

## 2. Ce que le RTS « vigilance client » ne fait pas

Le projet de RTS sur la vigilance client, établi au titre de l'article 28(1) de l'AMLR, a fait l'objet d'une consultation publique du 9 février au 8 mai 2026. La version soumise à consultation ne contient pas de section dédiée aux adresses auto-hébergées : elle fixe un cadre horizontal (informations d'identification, sources fiables de vérification, objet et nature de la relation d'affaires ou de la transaction, source et destination des fonds, mesures simplifiées ou renforcées, dépistage des sanctions financières ciblées).

C'est précisément pour cette raison que l'INBi a répondu à la consultation le 8 mai. Non pour demander une exemption, mais pour éviter que ce standard horizontal soit appliqué, dans le cas d'un client déjà identifié retirant vers une adresse dont il établit le contrôle, comme une obligation de collecter davantage que nécessaire.

Ce silence n'est pas nécessairement une omission. Il correspond à l'architecture du règlement : le régime dédié aux adresses auto-hébergées se trouve à l'article 40 de l'AMLR. L'AMLA indique d'ailleurs avoir veillé à ce

que le projet de RTS reste silencieux là où l'AMLR est déjà suffisamment détaillé (« remain silent where the AMLR is sufficiently detailed »). Le RTS vigilance client n'avait donc pas vocation à dupliquer ce régime.

Mais ce silence a aussi une conséquence opérationnelle. Le régime auquel il renvoie existe (c'est l'article 40), mais il ne s'appliquera qu'en juillet 2027, et les critères concrets de son application, attendus des orientations de l'AMLA, ne sont pas encore écrits : un renvoi vers des critères qui restent à écrire n'est pas une borne. Dans l'intervalle, les services conformité appliqueront les règles horizontales ; c'est là que se situe le risque de surcollecte défensive. Un texte horizontal qui ne dit rien du cas nominal (un client déjà identifié qui retire vers une adresse dont il prouve le contrôle) laisse chaque prestataire arbitrer seul, et l'arbitrage est biaisé : collecter trop peu l'expose à une sanction du superviseur ; collecter trop n'expose, en pratique, que ses clients (mécanisme documenté dans notre note d'avril 2026).

Il faut dire pourquoi cet enjeu, d'apparence procédurale, n'en est pas un. Les données en cause ne sont pas des données ordinaires : associer une identité civile, une adresse et un historique de transactions en crypto-actifs, c'est constituer un fichier qui indique où vivent des personnes et ce qu'elles détiennent. Ces fichiers finissent par fuiter, les précédents ne manquent pas, et, une fois dans de mauvaises mains, ils servent à cibler physiquement des détenteurs et leurs proches. Notre note d'avril 2026 documentait cette chaîne : le caractère durablement exploitable d'une fuite de données patrimoniales, et la concentration en France des agressions visant des détenteurs de crypto-actifs. Chaque donnée collectée sans nécessité n'est donc pas un simple coût administratif : c'est un risque créé, persistant, à la charge de personnes qui ne sont soupçonnées de rien.

Le problème n'est donc pas que le RTS du 10 juillet créerait une règle cachée contre la conservation en propre. Le problème est inverse : son silence peut laisser prospérer des pratiques maximales, faute de borne explicite.

## 3. Ce qui viendra en 2027 : l'article 40 AMLR

Le régime dédié se trouve à l'article 40 de l'AMLR. Il impose aux CASP d'identifier et d'évaluer les risques de blanchiment et de financement du terrorisme liés aux transferts vers ou depuis des adresses auto-hébergées, puis d'appliquer des mesures d'atténuation.

Le texte est décisif sur deux expressions : les mesures doivent être « proportionnées aux risques identifiés » et comprennent « l'une ou plusieurs » des actions énumérées. Autrement dit, l'article 40 ne pose pas une mesure automatique ni maximale. Il impose une réponse, mais en organise la gradation : identification et vérification fondées sur les risques de l'initiateur ou du bénéficiaire, renseignements supplémentaires sur l'origine ou la destination des crypto-actifs, surveillance continue renforcée, ou autres mesures d'atténuation, notamment contre le contournement des sanctions financières ciblées.

Deux conséquences s'ensuivent. D'abord, la conservation en propre n'est pas traitée comme une exemption : elle entre bien dans le champ LBC-FT. Ensuite, le texte ne pose pas une présomption de collecte maximale : il parle d'évaluation, de risque identifié et de proportionnalité.

L'AMLA doit émettre, au plus tard le 10 juillet 2027, un an jour pour jour après la soumission des premiers RTS, des orientations précisant ces mesures, notamment les critères et moyens d'identification et de vérification, ainsi que les critères permettant d'établir si une adresse auto-hébergée est détenue ou contrôlée par un client. Au 8 juillet 2026, la page officielle des instruments réglementaires de l'AMLA ne faisait apparaître aucun chantier consacré à l'article 40(2), sous réserve de la mention selon laquelle cette page n'est pas exhaustive. Aucun appel à contribution public sur ce régime n'a été identifié. La fenêtre utile reste donc devant nous.

L'échéance de juillet 2026 compte pour le socle horizontal : c'est lui qui encadrera la pratique quotidienne des prestataires. Pour le régime dédié, la partie se joue dans la séquence des orientations de l'article 40(2), attendues d'ici juillet 2027 ; une séquence qui, si elle suit la pratique de l'AMLA pour ses autres instruments, passera par une consultation publique.

## 4. La pièce d'évaluation manquante

Le TFR prévoit aussi un rapport de la Commission sur les risques posés par les transferts vers ou depuis des adresses auto-hébergées et sur l'opportunité de mesures spécifiques (article 37(2)). L'échéance était fixée au 1er juillet 2026. À la date de la présente note, aucun rapport n'a été identifié dans les sources officielles consultées.

L'INBi n'en tire pas un argument d'illégalité. Ce rapport n'est pas une condition de validité du RTS vigilance client, ni une condition d'existence de l'article 40 AMLR. Mais il est la pièce prévue pour apprécier, sur données, si des mesures supplémentaires sont justifiées. Toute orientation de 2027 sur les adresses auto-hébergées devrait donc intégrer cette évaluation et en discuter la méthode. C'est l'ordre normal d'un test de nécessité : démontrer le besoin avant de calibrer la contrainte.

## 5. Le bon test : ni exemption, ni collecte indifférenciée

La lutte contre le blanchiment et le financement du terrorisme est un objectif légitime. La question n'est pas le but poursuivi, mais la proportionnalité des moyens.

Ce que portent les textes existants tient en une phrase : ils autorisent des contrôles ; ils ne justifient pas une collecte indifférenciée lorsque le risque faible est documenté.

Par cas nominal, on entend ici le retrait d'un client déjà identifié vers une adresse dont il établit le contrôle, sans indice objectif de risque additionnel.

Trois bornes devraient être inscrites dans les textes d'application ou, a minima, dans la doctrine de supervision :

1. Le recours à une adresse auto-hébergée ne suffit pas, à lui seul, à justifier une collecte additionnelle ou une mesure renforcée.
2. Si le client est déjà identifié et si le contrôle de l'adresse est vérifié et documenté, le prestataire a satisfait le besoin d'identification du cas nominal. Des informations supplémentaires ne devraient être demandées qu'en présence d'un indice objectif qui fait sortir l'opération de ce cas.
3. L'absence de collecte additionnelle, dans un cas nominal documenté et de faible risque, ne devrait pas être traitée comme une défaillance de vigilance.

Ces bornes ne créent aucun régime de faveur. Elles traduisent l'approche par les risques que les textes revendiquent déjà, et prolongent ce que les orientations EBA admettent dès aujourd'hui : une vérification documentée dans les systèmes, une inscription sur liste blanche possible, un retrait si le risque ou le contrôle change, et aucune mesure renforcée automatique du seul fait qu'un transfert implique une adresse auto-hébergée.

Ces bornes n'ignorent pas les limites du dispositif : une adresse auto-hébergée peut opérer sans aucun intermédiaire assujetti, être contrôlée conjointement, ou être transmise après vérification. C'est précisément pourquoi elles reposent sur le réexamen à partir d'indices objectifs plutôt que sur une collecte indifférenciée.

## 6. Ce qu'il faudra surveiller

Quatre rendez-vous diront si l'approche par les risques reste une méthode de calibrage ou devient, en pratique, une formule vide :

- le rapport final du RTS vigilance client, attendu autour de la soumission du 10 juillet 2026 : vérifier si un traitement des adresses auto-hébergées y a été introduit après consultation ;
- le rapport de la Commission prévu à l'article 37(2) du TFR : sa méthodologie d'évaluation des risques, et toute annonce de mesures spécifiques ou d'acte délégué ;
- l'ouverture du chantier des orientations de l'article 40(2) AMLR : c'est là que se jouera le régime dédié (avec, selon toute vraisemblance au vu de la pratique de l'AMLA, une consultation publique) ;
- les orientations sur la surveillance continue (article 26(5) AMLR, consultation ouverte jusqu'au 3 septembre 2026) : la surveillance renforcée étant l'une des mesures de l'article 40, la doctrine qui s'y fixera préfigure le traitement des transactions avec adresses auto-hébergées.

Pour l'INBi, ces quatre points appellent deux suites : une analyse à réception des documents finaux, puis une contribution dédiée à l'ouverture du chantier des orientations de l'article 40(2).

## Conclusion

Le 10 juillet 2026 ne ferme donc pas le dossier des adresses auto-hébergées. Il fixe une partie du socle horizontal de vigilance client. Le régime dédié, lui, relève de l'article 40 de l'AMLR : il s'appliquera en 2027 et ses orientations restent à écrire.

La séquence utile est donc devant nous. L'INBi y portera la même ligne que dans sa contribution de mai : pas d'exemption, mais pas de collecte par réflexe. Lorsqu'un client est identifié, que le contrôle de l'adresse est vérifié et qu'aucun indice objectif ne fait sortir l'opération du cas nominal, le prestataire doit pouvoir documenter cette situation sans demander davantage.

Sans cette borne, le silence du texte ne restera pas neutre. Il sera rempli par les services conformité, et il le sera dans le sens le plus défensif : collecter plus pour ne jamais avoir à expliquer pourquoi l'on a collecté moins. Or, notre note d'avril le documentait, collecter plus, c'est protéger moins.

## Sources


1. AMLA, *Consultation on the draft RTS on Customer Due Diligence* (ouverte le 9 février 2026, close le 8 mai 2026 ; page indiquant « Results will follow » au 7 juillet 2026) : https://www.amla.europa.eu/policy/public-consultations/consultation-draft-rts-customer-due-diligence_en
2. AMLA, *Consultation Paper — Draft RTS under Article 28(1) of Regulation (EU) 2024/1624*, 9 février 2026 (dont la mention « remain silent where the AMLR is sufficiently detailed ») : https://www.amla.europa.eu/document/download/3d430294-5171-455c-b565-a86fc5f3cb1c_en?filename=Consultation+Paper+Draft+RTS+under+Article+28%281%29.pdf
3. AMLA, *Regulatory Instruments* (consultée en dernier lieu le 8 juillet 2026) : https://www.amla.europa.eu/policy/regulatory-instruments_en
4. EBA, *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers* (EBA/GL/2024/11, 4 juillet 2024 ; application 30 décembre 2024). EN : https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf ; FR : https://www.eba.europa.eu/sites/default/files/2024-09/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines_Final%20Report%20%28EBA.GL_.2024.11%29_FR_COR.pdf
5. Règlement (UE) 2024/1624 (AMLR), art. 40 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32024R1624 *(texte consulté le 7 juillet 2026)*
6. Règlement (UE) 2023/1113 (TFR), art. 14(5), 16(2), 36 et 37(2) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R1113 *(texte consulté le 7 juillet 2026)*
7. INBi, *Collecter plus, protéger moins ?*, note de recherche, 19 avril 2026 : https://inbi.fr/collecter-plus-proteger-moins-amlr-tfr/
8. INBi, *Consultation AMLA : l'INBi défend une application stricte de la proportionnalité aux règles visant les portefeuilles auto-hébergés*, 26 mai 2026 (contribution déposée le 8 mai 2026) : https://inbi.fr/consultation-amla-portefeuilles-auto-heberges/