

**Follow-up Committee on Manipulation of
Sports competitions
(T-MC)**

Council of Europe Convention on the
Manipulation of Sports Competitions
(CETS No. 215)



Strasbourg, 3 mars 2026

T-MC(2025)5rev

Comité de suivi sur la manipulation de compétitions sportives

**Convention du Conseil de l'Europe sur la manipulation
des compétitions sportives (STCE n° 215)**

**Lignes directrices sur la prévention et la lutte contre le
blanchiment d'argent lié aux paris sportifs**

TABLE DES MATIERES

Résumé exécutif	3
Introduction.....	4
1. Le blanchiment d'argent au cœur du fonctionnement des organisations criminelles	4
2. Une activité aux formes multiples	4
3. Un marché des paris sportifs en pleine expansion	4
4. Une priorité croissante pour les autorités européennes	4
5. Lien entre manipulation sportive et blanchiment d'argent	5
6. Objectif de ce document	5
Les facteurs de vulnérabilité du marché des paris sportifs au blanchiment d'argent	5
1. Un marché fluide et transnational, terrain idéal pour le blanchiment d'argent.....	5
2. Les moyens de paiement anonymes facilitent le blanchiment.....	6
3. Des failles réglementaires et des juridictions peu coopératives exploitées par certains opérateurs.....	6
Typologies et évaluation des risques.....	7
1. Les paris physiques restent une cible pour le blanchiment	7
2. Risques accrus sur les plateformes de paris en ligne	8
3. Crypto-actifs et blanchiment dans les paris en ligne	9
Limites des dispositifs actuels de lutte contre le blanchiment dans les paris sportifs	10
1. Des cadres de régulation encore insuffisants	10
2. Le rôle ambivalent de certains opérateurs de paris.....	11
3. Faiblesses dans la mise en œuvre des mesures de vigilance à l'égard de la clientèle (CDD)	11
4. Des déclarations des transactions suspectes encore trop rares	11
5. Les défis posés par les actifs virtuels	12
6. Trop peu d'enquêtes et de poursuites	12
Conclusion	13
1. Renforcement des mesures nationales de prévention et de détection	13
2. Importance d'une coopération internationale pour améliorer les dispositifs	15
Annexe 1 : Evaluation des risques pour les marchés physiques	16
Annexe 2 : Evaluation des risques pour les plateformes en ligne	17
Annexe 3 : Mesures en lien avec la 6e directive européenne anti-blanchiment.....	18

RESUME EXECUTIF

Le blanchiment d'argent continue d'alimenter la criminalité organisée

Il peut soutenir des activités criminelles motivées par le profit, financer le terrorisme et constitue, en soi, une activité lucrative. Il est estimé qu'entre 800 milliards et 2 000 milliards de dollars américains sont blanchis chaque année dans le monde (ONUDC, 2021).

L'Union européenne a récemment renforcé son cadre réglementaire, mais des vulnérabilités persistent — notamment dans le secteur des paris sportifs.

Le marché des paris présente plusieurs caractéristiques à haut risque

Il est vaste, très dynamique et hautement fluide. Les transactions y sont rapides, parfois transfrontalières, et réalisées via de nombreuses plateformes.

Certaines caractéristiques des comptes de paris — notamment les mouvements rapides de fonds, l'utilisation de multiples comptes et la diversité des moyens de paiement — créent des opportunités pour dissimuler les flux financiers.

Par ailleurs, certains opérateurs sont établis dans des juridictions où les exigences de supervision sont limitées ou inégales. Les groupes criminels exploitent ces failles, soit en détournant des services existants, soit en mettant en place leurs propres structures pour blanchir des fonds illicites.

La diversité des types de paris facilite la dissimulation

Avec une grande diversité de formats (notamment les paris en direct, les paris à cote fixe, les paris entre particuliers, les spread betting, les paris sur des événements mineurs, etc.), il existe de nombreuses façons de fragmenter les mises et de brouiller les pistes.

Parier sur des issues opposées (« surebet ») ou utiliser plusieurs comptes peut également permettre de simuler des pertes ou de répartir les gains, rendant les flux financiers plus difficiles à retracer.

Certaines méthodes de paiement renforcent l'anonymat

Certains canaux de paiement, tels que les cartes prépayées, les vouchers/bons, les portefeuilles électroniques (e-wallets) ou certains crypto-actifs, permettent de déposer ou de transférer des fonds avec une transparence limitée, selon la manière dont les procédures de vérification et de vigilance sont appliquées.

Les transactions peuvent être effectuées rapidement, parfois sous forme de petits montants répétés ou via plusieurs plateformes, ce qui complique l'identification de l'origine des fonds.

Les contrôles restent insuffisants

Les obligations de vigilance à l'égard de la clientèle (Customer Due Diligence)¹ existent dans la plupart des juridictions, mais leur mise en œuvre demeure inégale. Les déclarations d'opérations suspectes (DOS/SAR) sont insuffisantes ou tardives, et les enquêtes de suivi restent limitées dans de nombreuses juridictions.

Le manque de ressources spécialisées et la concurrence entre priorités affaiblissent l'attention portée aux flux financiers, tandis qu'une coopération internationale limitée entrave également l'efficacité de l'action.

Des solutions existent pour mieux prévenir et agir

Le rapport recommande plusieurs mesures au niveau national : renforcer les contrôles d'identité, encadrer les moyens de paiement, améliorer la supervision des opérateurs et faciliter le partage d'informations avec les institutions financières. Il appelle également à une meilleure détection des comportements atypiques et à un suivi plus strict des comptes à haut risque.

Au niveau international, il encourage un renforcement de la coopération entre les cellules de renseignement financier, les autorités de régulation et les services répressifs. L'objectif est de mieux identifier les détournements du secteur et d'en réduire l'attractivité pour le blanchiment d'argent.

¹ Vigilance à l'égard de la clientèle (Customer Due Diligence – CDD) : contrôles fondés sur les risques portant sur les clients, incluant la vérification de leur identité, la compréhension de leur profil et l'examen des transactions afin de détecter des activités inhabituelles.

INTRODUCTION

1. Le blanchiment d'argent au cœur du fonctionnement des organisations criminelles

Le blanchiment de capitaux est une activité centrale qui facilite la criminalité organisée, le financement du terrorisme et, plus largement, diverses activités économiques illicites. Il désigne le processus par lequel les produits d'activités criminelles sont dissimulés afin de leur donner une apparence légitime (MONEYVAL)². Une fois blanchis, ces fonds peuvent être réinjectés dans l'économie légale via des investissements dans des entreprises ou des montages financiers, ce qui contribue à masquer davantage leur origine réelle.

Ce phénomène est en forte expansion et s'inscrit de plus en plus dans une dynamique mondiale. Des estimations internationales largement citées évaluent le blanchiment de capitaux à 2 à 5 % du PIB mondial, ce qui représente un montant pouvant atteindre 2 000 milliards de dollars par an (ONUDD)³. Face à cette menace, l'Union européenne a adopté un nouveau paquet législatif en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT – AML/CFT)⁴, visant à renforcer la cohérence et l'efficacité de cette lutte entre les États membres.

2. Une activité aux formes multiples

Le blanchiment d'argent est un domaine d'activité criminelle autonome, en constante mutation. Il peut varier en complexité et en sophistication, allant de méthodes simples à des montages impliquant des structures juridiques, des sociétés écrans ou des opérations transfrontalières (Organised Crime in Australia, 2017)⁵.

Les criminels ciblent des secteurs ou des mécanismes qui maximisent les chances de dissimulation, notamment des espaces faiblement régulés, les plateformes numériques ou les systèmes de paiements anonymes. Ils peuvent également exploiter les différences entre les cadres nationaux de LCB/FT (AML/CFT).

3. Un marché des paris sportifs en pleine expansion

Au cours des trente dernières années, le marché mondial des paris sportifs — défini comme une mise monétaire dans l'espoir d'un gain dépendant de la réalisation d'un événement incertain lié à une compétition sportive⁶ — a profondément évolué en termes d'échelle et de nature.

Selon les Nations Unies (ONUDD, 2021)⁷, le montant total des mises annuelles pourrait dépasser 1 400 milliards de dollars. La clandestinité, illégalité d'une partie des flux, l'absence d'une régulation harmonisée et la complexité des opérations (transferts de mises, techniques de couverture) rendent l'évaluation globale difficile.

Dans ce contexte, les comptes des parieurs présentent des vulnérabilités comparables à celles observées pour des comptes financiers soumis à une supervision limitée ou appliquée de manière inégale.

Des affaires récentes en Australie⁸ et au Royaume-Uni⁹ illustrent que de telles vulnérabilités peuvent apparaître dans n'importe quelle juridiction, ce qui souligne la nécessité d'une mise en œuvre cohérente des obligations de LCB/FT (AML/CFT) dans l'ensemble des juridictions.

4. Une priorité croissante pour les autorités européennes

En 2022, la Commission européenne (SNRA – *Supranational Risk Assessment* 2022)¹⁰ a publié son rapport d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme. Le secteur des jeux d'argent, y compris les paris, y est classé

² MONEYVAL en bref (voir [ici](#)) : il s'agit de l'organisme régional de type GAFI du Conseil de l'Europe, chargé d'évaluer le respect, par les États membres non évalués directement par le GAFI, des normes internationales en matière de LCB/FT (AML/CFT).

³ MONEYVAL (2023a), Rapport annuel 2022 (disponible [ici](#)) ; ou entre 800 et 2 000 milliards de dollars selon l'ONUDD (s. d.), Blanchiment de capitaux (disponible [ici](#)).

⁴ LCB/FT (Lutte contre le blanchiment de capitaux et le financement du terrorisme) / AML/CFT : désigne l'ensemble des mesures juridiques, réglementaires et institutionnelles visant à prévenir et détecter le blanchiment de capitaux et le financement du terrorisme.

⁵ Commission australienne du renseignement criminel (2017), Le crime organisé en Australie 2017 (disponible [ici](#)).

⁶ Conseil de l'Europe, Convention sur la manipulation de compétitions sportives (Convention de Macolin), art. 3.

⁷ Le produit brut des jeux (PBJ) annuel, indicateur plus pertinent, est estimé à environ 65 milliards d'euros par an (CK Consulting)

⁸ Commission australienne des valeurs mobilières et des investissements (2023), Star fournit 150 millions de dollars pour les amendes et les pénalités après que l'ASIC a fait part de ses préoccupations (disponible [ici](#)) ; Reuters (2023), Un tribunal australien approuve une amende de 300 millions de dollars pour blanchiment d'argent pour Crown Resorts de Blackstone (disponible [ici](#)).

⁹ Commission des jeux de hasard (2023), £6.1m fine for online operator In Touch Games (disponible [ici](#)) ; Commission des jeux de hasard (2022), £9.4m fine for online operator 888 (disponible [ici](#)).

¹⁰ Commission européenne (2022), Rapport de la Commission au Parlement européen et au Conseil relatif à l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontalières (disponible [ici](#)).

au niveau de risque le plus élevé. L'évaluation nationale des risques 2023 de la UK Gambling Commission classe également les paris à distance (en ligne) et les paris en points de vente physiques comme des activités présentant un niveau élevé de risque de blanchiment de capitaux et de financement du terrorisme, les plaçant parmi les produits de jeux nécessitant les garanties les plus strictes.

Un rapport scientifique de l'institut [Transcrime](#) (Nazzari et Riccardi, 2024), fondé sur les données policières italiennes, montre que les jeux et paris sont devenus le premier secteur d'investissement des mafias italiennes pour des activités de blanchiment.

5. Lien entre manipulation sportive et blanchiment d'argent

L'article 16.3 de la Convention de Macolin prévoit explicitement que la manipulation des compétitions doit être prise en compte dans les dispositifs de prévention du blanchiment de capitaux, en imposant aux opérateurs de paris des obligations de vigilance, de conservation des données et de déclaration.

L'ONUDC¹¹ indique que la manipulation d'événements sportifs génère des produits criminels qui sont fréquemment intégrés au système financier via des comptes de paris et d'autres mécanismes de paiement.

6. Objectif de ce document

Ce document offre une vue d'ensemble des risques de blanchiment d'argent liés aux paris sportifs, afin de mieux comprendre leur nature, leur ampleur et leurs dynamiques. Il présente également un ensemble de recommandations visant à renforcer les capacités de prévention, de détection et d'enquête.

LES FACTEURS DE VULNERABILITE DU MARCHE DES PARIS SPORTIFS AU BLANCHIMENT D'ARGENT

1. Un marché fluide et transnational, terrain idéal pour le blanchiment d'argent

Les blanchisseurs d'argent privilégient les marchés à forts chiffres d'affaires, dynamiques et difficiles à réguler. Le secteur des jeux d'argent est utilisé à cette fin depuis de nombreuses années (James Banks, 2017)¹².

Le marché mondial des paris est particulièrement vulnérable en raison de sa grande fluidité — accessibilité transfrontalière, rapidité des opérations et prolifération des plateformes (Organised Crime in Australia, 2017)¹³. Les parieurs peuvent placer des mises dans plusieurs juridictions. Le niveau de contrôle appliqué à l'activité de paris varie fortement selon le cadre juridique et le dispositif de supervision en place.

La grande diversité des options de paris — paris en direct, cotes fixes, betting exchanges, paris sur des événements spécifiques d'une rencontre (spot betting)¹⁴, paris-fourchettes (spread betting)¹⁵ — multiplie les opportunités de dissimuler des flux illicites (Gambling Commission, 2020)¹⁶. Certaines techniques, telles que les paris sur des issues opposées ou les paris entre particuliers, facilitent la collusion et peuvent compliquer la détection de flux atypiques.

Les innovations technologiques, notamment les paris liés aux NFTs (Non-Fungible Tokens)¹⁷, au Metaverse¹⁸ et au Web3¹⁹, accentuent encore les risques en contournant les réglementations traditionnelles (Purbrick, 2023²⁰). L'usage de comptes multiples ou

¹¹ ONUDC, *Rapport mondial sur la corruption dans le sport* (2021), Office des Nations Unies contre la drogue et le crime.

¹² James Banks, *Gambling, Crime and Society* (London: Palgrave Macmillan, 2017).

¹³ Commission australienne du renseignement criminel (2017), *Le crime organisé en Australie 2017* (disponible [ici](#)).

¹⁴ Pari placé sur un événement ou une action très précise et isolée au cours d'un match (ex. : premier corner, prochain carton jaune), souvent en direct, ce qui en fait un format particulièrement vulnérable à la manipulation.

¹⁵ Forme de pari où le gain ou la perte dépend de l'écart entre le résultat réel d'un événement (ex. : nombre de buts ou corners) et une fourchette prédéfinie par l'opérateur, multiplié par la mise par unité d'écart.

¹⁶ Gambling Commission (2023), *The Money Laundering and Terrorist Financing Risks within the British Gambling Industry* (Les risques de blanchiment d'argent et de financement du terrorisme dans l'industrie du jeu britannique) (disponible [ici](#)).

¹⁷ Jetons numériques uniques inscrits sur une blockchain, utilisés dans certains paris pour représenter des objets virtuels ou des enjeux dont la valeur dépend d'événements sportifs.

¹⁸ Environnements virtuels immersifs en 3D où les utilisateurs peuvent interagir, jouer ou parier, souvent via des crypto-monnaies, en dehors de toute réglementation traditionnelle.

¹⁹ Nouvelle génération d'applications décentralisées basées sur la blockchain, permettant des paris via des contrats intelligents sans intervention d'un opérateur central ni contrôle réglementaire.

²⁰ Martin Purbrick (2023). *Le déplacement des paris illégaux et de la criminalité organisée transnationale*. Asian Racing Federation (ARF) – Bulletin du Council on Anti-Illegal Betting and Financial Crime, Bulletin trimestriel, février 2023 (disponible [ici](#)).

VIP, peu encadrés, permet de masquer l'origine des fonds (Moneyval, 2013²¹). Enfin, une concurrence intense pousse les opérateurs à augmenter les taux de retour aux joueurs, réduisant ainsi le coût du blanchiment (Precrimbet, 2017)²².

2. Les moyens de paiement anonymes facilitent le blanchiment

Au-delà des caractéristiques du marché lui-même, les méthodes de paiement constituent une vulnérabilité majeure. Il est possible de placer de grosses mises de façon anonyme, notamment lorsque les opérateurs échappent à une supervision effective ou opèrent depuis des juridictions où le contrôle AML/CFT (lutte contre le blanchiment et le financement du terrorisme) est limité (Organised Crime in Australia, 2017). Ces opérateurs proposent souvent des plafonds de mise élevés, en particulier pour les VIP, sans appliquer de contrôles rigoureux de vérification d'identité.

Les blanchisseurs recourent aussi à des mules financières ou à des intermédiaires afin de dissimuler l'origine et la propriété des fonds. L'utilisation de cartes prépayées, de bons/ vouchers²³, de portefeuilles électroniques (e-wallets) ou de plateformes de paiement insuffisamment surveillées complique encore la traçabilité (Moneyval, 2013).

Une affaire récente a mis au jour l'usage de prestataires de services de paiement tels que Neteller, Skrill et Western Union dans une opération transfrontalière de blanchiment, où les fonds circulaient à l'aide de faux documents d'identité.

Les crypto-monnaies comme Monero ou Zcash offrent, par conception, un haut degré d'anonymat²⁴. Europol (2020)²⁵ souligne que ces outils peuvent servir à alimenter des comptes de pari impliqués dans la manipulation sportive. Les prestataires de services sur actifs virtuels (VASPs) sont souvent difficiles à surveiller, en particulier lorsqu'il s'agit de flux transfrontaliers (Moneyval, 2023)²⁶. En réaction, des régulateurs comme la UK Gambling Commission ont relevé le niveau de risque associé aux crypto-actifs dans leurs évaluations AML/CFT.

Si la blockchain permet une traçabilité « théorique », les blanchisseurs utilisent fréquemment des plateformes d'échange, des altcoins²⁷ axés sur la confidentialité, des services de swap²⁸, ainsi que des services de mixing et de tumbling, ce qui rend l'origine des fonds difficile à établir (Europol, 2021).

Les paris sportifs et les crypto-monnaies partagent plusieurs caractéristiques : une croissance rapide depuis 2020, un recours massif aux canaux numériques, et des profils d'utilisateurs qui se recoupent souvent dans les environnements en ligne. Leur dimension spéculative et volatile renforce leur attractivité, mais aussi leur vulnérabilité à des usages détournés (Topps, 2023)²⁹.

Même si les crypto-monnaies restent marginales dans l'écosystème légal du traitement des paiements, elles sont largement utilisées dans les paris illégaux, notamment sur le Darknet, où l'anonymat et le contournement des contrôles sont la norme (Betmonitalert, 2017).

Les opérateurs illégaux sur le Darknet acceptent très majoritairement les crypto-monnaies. En 2023, un quart des sites de paris illégaux utilisaient des actifs virtuels, avec une forte prévalence du stablecoin Tether (USDT)³⁰ (ARF Council, 2024)³¹. Ces réseaux opèrent en dehors des systèmes classiques de vérification et permettent des transferts quasi anonymes à grande échelle.

3. Des failles réglementaires et des juridictions peu coopératives exploitées par certains opérateurs

La structure même du marché des paris constitue une vulnérabilité majeure. La coexistence des paris en ligne et en espèces crée des passerelles qui facilitent la dissimulation de l'origine illicite des fonds. En combinant ces deux canaux, les criminels peuvent intégrer des espèces issues d'activités illégales dans des circuits numériques, où la traçabilité devient plus complexe. Plusieurs

²¹ MONEYVAL (2013). *L'utilisation des jeux d'argent en ligne à des fins de blanchiment de capitaux et de financement du terrorisme*. Conseil de l'Europe, Rapport de recherche typologique, avril 2013.

²² Precrimbet. (2017). Prévenir les risques criminels liés au marché des paris sportif (disponible [ici](#)).

²³ Voucher : bon d'achat ou code prépayé, souvent acquis en espèces, permettant de créditer un compte en ligne sans passer par un compte bancaire ou une carte nominative.

²⁴ Privacy coins : crypto-monnaies dites « confidentielles » conçues pour garantir l'anonymat total ou renforcé des transactions. Elles utilisent des technologies comme le masquage des adresses ou le chiffrement des montants, ce qui les rend particulièrement attractives pour des usages illicites, notamment le blanchiment d'argent.

²⁵ Europol (2021). L'implication des groupes criminels organisés dans la corruption sportive (disponible [ici](#)).

²⁶ Moneyval (2023b), Risques de blanchiment d'argent et de financement du terrorisme dans le monde des actifs virtuels (disponible [ici](#)).

²⁷ Altcoin : terme générique désignant toute crypto-monnaie autre que le Bitcoin. Certains altcoins, appelés « privacy coins », intègrent des fonctionnalités de confidentialité renforcée qui compliquent la traçabilité des transactions.

²⁸ Service de swap : plateforme permettant d'échanger rapidement une cryptomonnaie contre une autre, sans passer par un échange centralisé ni créer de compte. Ces services, souvent non régulés, sont utilisés pour fragmenter et obscurcir les flux financiers lors d'opérations de blanchiment.

²⁹ Topps, A. (2023), Placez vos paris : L'intégration juridique des paris sportifs avec les crypto-monnaies, *UNH Sports Law Review*, 2(1), 5 (disponible [ici](#)).

³⁰ Tether (USDT) : stablecoin, c'est-à-dire une crypto-monnaie dont la valeur est indexée sur une monnaie fiduciaire (en l'occurrence le dollar américain). Il est largement utilisé dans les transactions crypto en raison de sa stabilité relative, y compris sur des plateformes de jeux d'argent et de paris non réglementées, qui opèrent illégalement.

³¹ Conseil de l'ARF (2024), Comment les paris illégaux et le blanchiment d'argent connexe ont prospéré malgré "l'hiver des crypto-monnaies" (disponible [ici](#)).

enquêtes ont mis en lumière des réseaux exploitant simultanément des boutiques physiques et des sites de paris en ligne contrôlés par les mêmes groupes criminels (Precrimbet, 2017³²).

De nombreux opérateurs sont établis dans des juridictions où les exigences en matière de LBC/FT (AML/CFT) sont faibles et où la surveillance réglementaire est limitée.

Certains dispositifs d'agrément, tels que les modèles « white label », nécessitent des clarifications, mais la responsabilité de la conformité LBC/FT demeure juridiquement assumée par le titulaire de la licence au regard des règles de la UK Gambling Commission³³.

Selon la Commission australienne du renseignement criminel (2017), les bookmakers privilégient des juridictions peu régulées et peu coopératives avec les autorités étrangères. L'absence de réglementation homogène et la nature transnationale des paris en ligne en font un canal particulièrement efficace pour le blanchiment et le financement d'activités criminelles (Conseil de l'ARF, 2023). Des représentants des forces de l'ordre dénoncent également le manque de coopération de certains territoires offshore, qui ignorent souvent les demandes d'assistance juridique.

Mettre en place un site de paris dans le but de blanchir de l'argent est relativement simple dans les juridictions où les exigences d'agrément, les obligations de CDD (vigilance à l'égard de la clientèle / *Customer Due Diligence*) et les contrôles LBC/FT (AML/CFT) sont faibles, voire inexistantes. Cependant, des opérateurs tiers peuvent également exploiter des contrôles insuffisants pour dissimuler des flux financiers illicites. Leur implantation dans des juridictions offshore rend les enquêtes complexes en raison de structures opaques : sociétés écrans, comptes bancaires fragmentés, serveurs situés à l'étranger et délocalisations fréquentes d'une juridiction à l'autre (Purbrick, 2023)³⁴.

Plus largement, les sites de paris peuvent être conçus spécifiquement pour le blanchiment ou servir de relais à des blanchisseurs extérieurs. Leur grande flexibilité opérationnelle, conjuguée à l'absence de transparence sur les bénéficiaires effectifs et à la facilité de contourner les règles nationales (forum shopping), favorise leur exploitation par les groupes criminels. Cette évolution illustre la capacité du crime organisé à intégrer des structures légales à ses opérations et à adapter en permanence ses méthodes aux environnements réglementaires (Europol, 2021).

TYPLOGIES ET EVALUATION DES RISQUES

1. Les paris physiques restent une cible pour le blanchiment

Les marchés de paris en point de vente, reposant sur des réseaux physiques de distribution, sont souvent considérés comme moins exposés aux formes de blanchiment les plus sophistiquées que les casinos ou les plateformes en ligne. Cependant, l'importance des opérations en espèces, l'anonymat de certaines transactions et la multiplicité des points de vente continuent de créer des vulnérabilités.

Le recours à l'argent liquide, l'anonymat des opérations et la possibilité de placer de nombreux paris de faible montant dans différents points de vente permettent l'introduction de produits d'origine criminelle³⁵.

Ces risques sont particulièrement marqués dans les juridictions où la surveillance des points de vente est limitée ou lorsque la vigilance à l'égard de la clientèle est appliquée de manière inégale.

Des pratiques telles que les paiements sans contact ou l'utilisation d'appareils personnels (BYOD – Bring Your Own Device³⁶) compliquent encore la détection des flux illicites en fragmentant les transactions.

Une technique fréquemment utilisée est le smurfing, qui consiste à fractionner les mises ou les dépôts en petites transactions répétées afin d'éviter les seuils de déclaration ou les alertes automatiques. Ces opérations peuvent être réparties sur plusieurs établissements ou menées simultanément par différentes personnes, rendant les flux plus difficiles à retracer.

³² Precrimbet. (2017). *Prévenir les risques criminels liés au marché des paris sportifs* (disponible [ici](#)).

³³ Le système britannique de « white label » illustre les failles que certaines réglementations peuvent créer. Il permet aux titulaires de licences délivrées par la UK Gambling Commission de « louer » ces licences à des opérateurs tiers, parfois basés à l'étranger, sans que ces opérateurs ne soient soumis à des contrôles suffisants, notamment en matière de lutte contre le blanchiment de capitaux.

³⁴ Martin Purbrick (2023). *Le déplacement des paris illégaux et de la criminalité organisée transnationale*. Asian Racing Federation (ARF) – Bulletin du Council on Anti-Illegal Betting and Financial Crime, Bulletin trimestriel, février 2023 (disponible [ici](#)).

³⁵ Introduction d'espèces : première étape du blanchiment de capitaux, consistant à injecter des liquidités issues d'activités illégales dans l'économie ou dans le circuit financier légal. Dans le cas des paris sportifs, cela peut prendre la forme de l'achat de tickets ou de crédits, ou du dépôt d'espèces dans un point de vente, afin de transformer des fonds d'origine criminelle en gains apparemment légitimes.

³⁶ BYOD (Bring Your Own Device) : pratique consistant à permettre aux clients de placer des paris dans un point de vente physique à l'aide de leur propre téléphone mobile, sans créer de compte ni s'identifier, ce qui rend le suivi et la traçabilité des transactions difficiles.

La prise de contrôle ou l'influence de points de vente physiques par des réseaux de blanchiment peut également survenir dans certaines juridictions. Lorsque les exigences d'agrément, les inspections et les contrôles de l'actionnariat sont faibles, cette infiltration permet aux criminels d'opérer discrètement et de contourner les obligations internes de vigilance. Ces caractéristiques font des marchés de paris physiques un canal privilégié pour des formes de blanchiment d'argent discrètes mais efficaces.

Typologies principales :

- **Typologie 1 – Recycler de l'argent sale en rachetant des reçus de jeux gagnants**

Le blanchisseur organise un réseau de parieurs complices qui jouent avec de l'argent propre. Il leur rachète ensuite leurs gains en espèces d'origine illicite, puis encaisse les tickets à son nom. Pour retirer les fonds discrètement, il peut utiliser des services anonymes comme Hal Cash³⁷, qui permettent de retirer de l'argent sans compte bancaire identifié.

- **Typologie 2 – Utiliser des cartes bancaires volées pour parier**

Le criminel retire de l'argent avec une carte volée, place un pari, puis récupère ses gains sur son propre compte bancaire pour justifier l'origine des fonds.

- **Typologie 3 – Achat de bulletins gagnants anonymes**

Le blanchisseur approche un joueur gagnant (souvent avec la complicité de l'exploitant du point de vente), rachète son ticket en espèces en lui offrant une prime, puis encaisse les gains comme s'ils lui appartenaient.

L'évaluation des risques menée par la GB Gambling Commission (voir annexe 1) indique que les marchés terrestres présentent un niveau de risque global élevé, notamment en raison de mesures préventives insuffisantes (en particulier en matière de vigilance à l'égard de la clientèle / CDD), de vulnérabilités liées à l'usage de faux documents, de l'anonymat des transactions de paris (accentué par la prédominance des paiements en espèces) et de l'utilisation, faiblement encadrée, de multiples méthodes de paiement.

Dans l'ensemble, ces typologies montrent que les paris en point de vente conservent des vulnérabilités nettes au blanchiment de capitaux, en particulier du fait des transactions en espèces, des possibilités d'anonymat et de la dispersion de l'activité sur de nombreux points de vente. Les évaluations nationales des risques — dont celle de la UK Gambling Commission — classent ainsi les paris terrestres comme un secteur à haut risque pour ces raisons.

2. Risques accrus sur les plateformes de paris en ligne

L'absence d'interaction en face à face est reconnue de longue date comme un facteur compliquant la vérification de l'identité des clients dans les paris en ligne (vigilance à l'égard de la clientèle / CDD). Les évaluations antérieures, notamment Moneyval (2013), ont souligné ce risque et, même si les cadres technologiques et réglementaires ont évolué ces dernières années, ces vulnérabilités restent pertinentes dans certains environnements.

Dans certaines juridictions, des faiblesses telles que l'absence de contrôles de paiement en circuit fermé (*closed-loop*), une vérification insuffisante des comptes, ou la possibilité d'utiliser des comptes multiples ou fictifs accroissent l'exposition aux abus.

La complexité technique de ces plateformes peut aussi permettre à des groupes criminels d'en prendre le contrôle direct et d'y intégrer des flux illicites.

Des affaires récentes en Australie (Tabcorp, 2017 ; Star Entertainment, 2022) et au Royaume-Uni (William Hill, Coral, Ladbrokes, Star Sports) ont montré que même des opérateurs agréés peuvent présenter de graves faiblesses dans leurs mécanismes de détection³⁸. Ces exemples démontrent que des défaillances de vigilance client et de surveillance peuvent survenir même lorsqu'un cadre réglementaire existe. Ces insuffisances ont conduit à un renforcement des mesures de lutte contre le blanchiment³⁹. Les deux juridictions ont ensuite renforcé les obligations LBC/FT (AML/CFT), illustrant le rôle central de la supervision et de l'application des règles dans la réduction des risques.

³⁷ Halcash ([How it works](#)) : Service de transfert d'argent permettant d'envoyer des fonds à un numéro de téléphone mobile, que le destinataire peut retirer en espèces dans un distributeur automatique, sans avoir besoin de compte bancaire ni d'identification formelle. Ce système peut être détourné à des fins de blanchiment en facilitant des retraits anonymes.

³⁸ ABCNews (2022), L'organisme de surveillance contre le blanchiment d'argent enquête sur les géants des jeux d'argent en ligne Sportsbet et Bet365 (disponible [ici](#)) ; Racing Post (2023) ; Star Sports se voit infliger une amende de 594 000 £ pour manquements en matière de lutte contre le blanchiment d'argent et de responsabilité sociale (disponible [ici](#)).

³⁹ Casino Guardian. (2023), L'Austrac ordonne aux sociétés de paris sportifs en ligne de cesser d'accepter les mises de clients non vérifiés (disponible [ici](#)).

Typologies principales :

▪ Typologie 1 – Déposer de l'argent sale sur des plateformes pour encaisser des gains légitimes

Le blanchisseur ouvre un compte sur une plateforme de paris en ligne et y dépose des fonds issus d'activités criminelles, souvent via des moyens de paiement anonymes ou faiblement vérifiés. Il place ensuite des paris à faible risque (par exemple sur les favoris), ce qui lui permet de récupérer la majeure partie des fonds sous forme de gains. Ces gains, qui paraissent légitimes, sont alors transférés vers un compte bancaire personnel, donnant l'apparence de revenus licites. Le procédé est souvent répété via plusieurs comptes ou dans différentes juridictions afin d'obscurcir davantage l'origine des fonds.

Cette méthode de « jeu minimal » est bien documentée. Sa faisabilité est la plus élevée dans les juridictions où les obligations de vigilance (*CDD – Customer Due Diligence*) et de vigilance renforcée (*EDD – Enhanced Due Diligence*) sont limitées, ou lorsque les pratiques de vérification sont permissives.

▪ Typologie 2 – Création d'un site de paris pour intégrer des fonds illicites

Un réseau criminel met en place son propre site de paris sportifs, généralement hébergé dans une juridiction où la supervision AML/CFT est limitée, avec des faiblesses dans les mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Il recrute ensuite des complices, ou « mules », chargés de déposer des fonds sur des comptes de paris et de perdre volontairement des mises en pariant sur des issues improbables. Ces pertes sont alors transférées vers des comptes bancaires contrôlés par l'organisation criminelle, ce qui lui permet de récupérer les fonds sous un vernis de légalité.

L'évaluation des risques de la Gambling Commission britannique (voir annexe 2) confirme que les plateformes de paris en ligne sont exposées à des niveaux élevés de risque de blanchiment. Les principales vulnérabilités incluent l'utilisation de canaux de paiement « open-loop », des procédures de vigilance (*CDD – Customer Due Diligence*) insuffisantes, l'exposition liée aux comptes VIP, le multi-compte, ainsi qu'un large éventail de moyens de paiement numériques — dont certains permettent un degré élevé d'anonymat.

Même lorsque des contrôles existent et sont correctement appliqués, le niveau de risque demeure élevé. La rapidité des transactions, la diversité des produits de paris et la facilité de transférer des fonds d'une plateforme à l'autre continuent de créer des opportunités de dissimulation et d'abus.

3. Crypto-actifs et blanchiment dans les paris en ligne

Les crypto-monnaies sont de plus en plus utilisées comme outils de blanchiment d'argent, en particulier dans l'industrie du jeu en ligne. Leur anonymat relatif, combiné à la complexité technique de leur traçabilité, rend les enquêtes plus difficiles pour les autorités.

Cependant, les évolutions réglementaires de ces dernières années, notamment au sein de l'Union européenne, ont profondément remodelé cet environnement de risque. Le règlement (UE) 2023/1113 relatif aux transferts de fonds (la « travel rule ») impose désormais aux prestataires de services sur crypto-actifs de collecter et de transmettre, pour tout transfert, des informations sur l'initiateur et le bénéficiaire. Par ailleurs, le nouveau règlement anti-blanchiment (UE) 2024/1624 interdira les portefeuilles de crypto-actifs anonymes.

Les blanchisseurs d'argent utilisent généralement deux grands types de services pour manipuler des crypto-actifs⁴⁰ avant ou après leur passage par des plateformes de paris :

▪ Des services intermédiaires pour brouiller les pistes

Il s'agit notamment de portefeuilles non hébergés⁴¹ comme Metamask ou Trust Wallet, qui permettent de stocker des fonds sans passer par un « tiers de confiance », notamment sans vérification d'identité. Des mélangeurs⁴² comme Tornado Cash ou Sinbad sont utilisés pour rendre les transactions intraquables. Des marchés du darknet comme Hydra (fermé en 2022) permettent aussi d'échanger des crypto-actifs contre des biens ou services illicites. Ces services sont parfois utilisés en chaîne pour convertir, déplacer ou fragmenter les fonds avant d'alimenter des comptes de jeux.

▪ Passerelles vers la monnaie fiduciaire pour convertir les cryptos en euros, dollars et autres devises classiques

⁴⁰ Crypto-actif : terme générique désignant tout actif numérique reposant sur une technologie de registre distribué (comme la blockchain). Il inclut notamment les crypto-monnaies (ex. : Bitcoin), les stablecoins (ex. : Tether), les jetons utilitaires, les NFT ou encore les jetons de gouvernance. Ce terme est privilégié dans les textes réglementaires européens et internationaux.

⁴¹ Portefeuille non hébergé : application crypto gérée par l'utilisateur lui-même (ex. Trust Wallet, Metamask), sans passer par une plateforme centralisée. Elle ne requiert ni compte ni vérification d'identité.

⁴² Mélangeur (mixer) : service conçu pour masquer l'origine des fonds en mélangeant les crypto-actifs de plusieurs utilisateurs. Exemples : Tornado Cash (Ethereum), Sinbad (Bitcoin), ChipMixer (fermé).

Cette opération est souvent réalisée via des échanges centralisés comme Binance, Kraken ou Bitfinex, des plateformes peer-to-peer (P2P) comme Paxful ou LocalBitcoins (fermée en 2023), ou encore via des échanges décentralisés (DEX)⁴³ comme Uniswap ou PancakeSwap. Une fois les fonds convertis, ils peuvent être transférés vers des comptes bancaires ou retirés en espèces, échappant alors à la traçabilité de la blockchain. Ces passerelles sont parfois utilisées pour injecter des fonds dans des plateformes de paris.

Enfin, une tendance émergente réside dans l'utilisation de services clandestins, beaucoup plus discrets que les mélangeurs classiques. Ceux-ci ne sont accessibles que via des messageries privées (comme Telegram) ou le navigateur Tor, et ne sont annoncés que dans des forums spécialisés du darknet. Ces canaux permettent aux blanchisseurs d'alimenter des comptes de paris en ligne avec des fonds préalablement anonymisés, tout en échappant à la détection automatisée.

Un rapport de l'ONUDC (2024)⁴⁴ montre que des plateformes de paris illégales, notamment en Asie du Sud-Est, exploitent des crypto-monnaies comme le Tether (USDT) sur la blockchain TRON⁴⁵, devenue un outil central du blanchiment. Ces plateformes permettent de convertir et déplacer d'importants volumes d'argent sale, souvent liés au trafic de drogue, à la fraude ou à la cybercriminalité.

Typologies principales :

▪ Typologie 1 – Utiliser des comptes junkets⁴⁶ pour déplacer discrètement des fonds entre juridictions

Un joueur confie de l'argent à un intermédiaire de jeux (appelé junket) dans un pays. Cet argent n'est pas transféré directement vers un autre pays, mais crédité sur un compte interne du junket. Le joueur peut ensuite utiliser ce crédit dans un autre pays pour jouer dans un casino ou sur une plateforme liée. Ce système fonctionne en interne, par compensation entre les crédits et les pertes, sans mouvement bancaire international identifiable.

Certains junkets incitent même les clients à leur confier des fonds en offrant des taux d'intérêt élevés, ce qui les transforme en véritables banques parallèles, échappant à toute régulation financière.

▪ Typologie 2 – Mobiliser un réseau de comptes multiples pour fragmenter et faire transiter des fonds illicites

Des réseaux criminels recrutent des individus pour transférer de l'argent à leur place, en utilisant leurs propres comptes bancaires ou des comptes de jeu en ligne. Ces personnes, parfois appelées « fourmis mobiles », déplacent de petites sommes d'argent de manière répétée, entre plusieurs comptes ou plateformes. Elles ne sont pas toujours conscientes de l'origine illégale des fonds, mais agissent contre rémunération, souvent en recevant une commission pour chaque transfert.

Ce système est utilisé pour dissimuler l'identité des bénéficiaires effectifs ultimes et rendre la traçabilité des flux d'argent plus difficile. Il est souvent lié à des jeux illégaux, à des fraudes téléphoniques (par exemple des arnaques aux faux conseillers bancaires), ou à des activités criminelles organisées, comme le trafic de drogue ou la traite des êtres humains.

Globalement, les crypto-actifs continuent de présenter des risques importants de blanchiment de capitaux et de financement du terrorisme (BC/FT), en particulier dans des environnements opaques. Dans les juridictions réglementées, les réformes récentes de l'UE réduisent les vulnérabilités liées à l'anonymat, mais les groupes criminels continuent d'exploiter les lacunes de supervision, l'activité transfrontalière et les prestataires non conformes.

LIMITES DES DISPOSITIFS ACTUELS DE LUTTE CONTRE LE BLANCHIMENT DANS LES PARIS SPORTIFS

1. Des cadres de régulation encore insuffisants

Malgré la reconnaissance croissante des risques, les dispositifs actuels de lutte contre le blanchiment restent insuffisants. Si la plupart des États membres de l'UE imposent au secteur des paris de se conformer aux directives anti-blanchiment, l'évaluation de la mise en œuvre de la 4e directive par la Commission européenne a révélé des défaillances importantes.

⁴³ DEX (échange décentralisé) : plateforme d'échange de crypto-actifs fonctionnant sans autorité centrale. Elle permet d'effectuer des transactions directement entre utilisateurs, sans contrôle KYC. Exemples : Uniswap, PancakeSwap.

⁴⁴ ONUDC (janvier 2024), Casinos, blanchiment d'argent, banques souterraines et criminalité transnationale organisée en Asie de l'Est et du Sud-Est : Une menace cachée et croissante (disponible [ici](#)).

⁴⁵ Blockchain TRON : réseau blockchain décentralisé fondé en 2017, conçu pour des transactions rapides et à faible coût. Elle est largement utilisée pour le transfert de stablecoins, notamment Tether (USDT), en raison de ses faibles frais de transaction. Sa popularité dans les milieux illicites s'explique par l'anonymat relatif qu'elle offre, combiné à une grande accessibilité.

⁴⁶ Un "junket" est un accord entre un casino et un opérateur chargé de faciliter la venue et le jeu de joueurs fortunés, souvent dans le cadre de programmes VIP. Grâce à leurs liens avec les casinos, les opérateurs de junket peuvent offrir des avantages et des incitations à leurs membres ou à d'autres clients à haut revenu.

Dans plusieurs pays, il n'existe pas d'obligations spécifiques en matière de vérifications d'honorabilité⁴⁷ ou de compétence pour les bénéficiaires effectifs⁴⁸ lors de l'instruction des demandes d'agrément, ce qui permet à des acteurs liés au crime organisé d'opérer en toute légalité.

Le Royaume-Uni, de son côté, a mis en place des obligations spécifiques pour les opérateurs de paris, aussi bien en ligne que physiques, à travers des lignes directrices de la UK Gambling Commission⁴⁹. Toutefois, l'efficacité de ce dispositif dépend fortement de la mise en œuvre par les opérateurs, et certaines pratiques comme le système de marque blanche ont suscité des critiques pour leur manque de contrôle.

À l'échelle mondiale, le secteur souffre d'un manque de normes harmonisées en matière de LBC. L'absence de contrôles sur les bénéficiaires effectifs, la faiblesse des exigences de conformité, et le manque de surveillance des opérateurs notamment dans certaines juridictions offshore rendent difficile la détection, l'enquête et la poursuite des pratiques de blanchiment via les paris.

Cette fragmentation réglementaire crée des opportunités d'arbitrage réglementaire, les opérateurs choisissant des juridictions offrant une supervision minimale.

2. Le rôle ambivalent de certains opérateurs de paris

Les opérateurs de paris sont en première ligne dans la prévention du blanchiment de capitaux. Ils sont légalement tenus d'adopter une approche fondée sur les risques, de vérifier l'identité des clients, de mettre en place des dispositifs permettant de gérer et d'atténuer ces risques, d'allouer des ressources humaines et matérielles appropriées, et de déclarer les opérations suspectes.

Cependant, le niveau d'engagement des opérateurs varie fortement. Si certains opérateurs agréés appliquent des mesures LBC/FT, d'autres — notamment ceux opérant sur le Darknet ou sous licences offshore — mettent en œuvre peu, voire aucun contrôle. Dans certains cas, les blanchisseurs sont même perçus comme des clients rentables, car ils placent des mises importantes et acceptent certaines pertes. Dans ces environnements, les clients à forte dépense impliqués dans des activités suspectes peuvent faire l'objet de procédures de vérification plus légères ou d'une surveillance limitée, créant des situations où les incitations commerciales peuvent entrer en conflit avec les obligations de LBC/FT.

3. Des faiblesses dans la mise en œuvre des mesures de vigilance à l'égard de la clientèle (CDD/*Customer Due Diligence*)

L'efficacité des dispositifs de CDD (Know Your Customer) varie considérablement d'un opérateur à l'autre. Dans certains cas, les procédures d'identification sont soit insuffisantes, soit réalisées trop tardivement — par exemple au moment du retrait plutôt qu'au moment du dépôt — ce qui en réduit l'effet préventif.

L'évaluation des risques de la Gambling Commission britannique souligne que ces contrôles ne sont pas appliqués de manière constante. Cela s'explique notamment par le recours à des documents falsifiés⁵⁰, à de fausses identités ou à des techniques de « smurfing » (fractionnement des dépôts en montants plus faibles afin d'éviter les seuils de détection).

Par ailleurs, les opérateurs n'ont généralement qu'une vision partielle de l'activité de paris d'un client et ne peuvent pas accéder à des informations sur son comportement sur d'autres plateformes. Enfin, l'absence fréquente de systèmes de paiement en boucle fermée (« closed-loop »), dans lesquels la méthode de retrait est vérifiée et doit correspondre à la méthode de dépôt initiale, constitue une faiblesse en matière de traçabilité des flux financiers.

4. Des déclarations des transactions suspectes encore trop rares

Conformément à la législation européenne en matière de lutte contre le blanchiment de capitaux, tous les prestataires réglementés de services de jeux d'argent sont tenus de déclarer toute opération soupçonnée d'être liée au blanchiment de capitaux. Cette

⁴⁷ Vérifications d'honorabilité : procédures administratives ou judiciaires visant à s'assurer qu'une personne physique ou morale ne présente pas de risques en raison de condamnations pénales passées, de liens avec la criminalité organisée, ou d'antécédents compromettants. Dans le secteur des jeux, elles servent à empêcher que des individus liés à des activités illicites ne prennent le contrôle d'opérateurs agréés.

⁴⁸ Compétence des bénéficiaires effectifs : exigence visant à s'assurer que les personnes qui détiennent ou contrôlent effectivement une entreprise possèdent les connaissances, l'expérience et l'intégrité nécessaires pour exercer leurs responsabilités. Dans le secteur des jeux, cela permet de limiter les risques liés à une mauvaise gestion ou à une infiltration criminelle.

⁴⁹ GB Gambling Commission (2023), Prévention du blanchiment d'argent et lutte contre le financement du terrorisme, Gambling Commission guidance for remote and non-remote casinos (Directives de la Commission des jeux de hasard pour les casinos distants et non distants), Fifth edition, Revision 3, (disponible [ici](#)).

⁵⁰ La Gambling Commission du Royaume-Uni retient la définition du blanchiment de capitaux issue du *Proceeds of Crime Act* de 2002, selon laquelle un opérateur commet une infraction s'il accepte des fonds provenant d'une activité criminelle. Cela couvre à la fois les opérations visant à dissimuler l'origine des fonds et le simple fait d'utiliser des produits du crime pour effectuer des achats licites, y compris des jeux d'argent (disponible [ici](#)).

déclaration d'activité suspecte (SAR) est transmise à la cellule de renseignement financier par l'intermédiaire du responsable désigné, le MLRO (Money Laundering Reporting Officer).

Si cette obligation est clairement établie au niveau européen, son application reste inégale dans la pratique. Certains opérateurs tardent à effectuer les signalements, voire y renoncent, ce qui affaiblit l'efficacité du dispositif de prévention. Ce déficit peut s'expliquer par un manque de formation, une méconnaissance des indicateurs de risque, ou encore l'absence de retour d'information de la part des autorités compétentes.

5. Les défis posés par les actifs virtuels

Le GAFI (Groupe d'action financière)⁵¹ impose aux prestataires d'actifs virtuels (comme les plateformes de crypto-monnaies) d'être enregistrés, agréés et surveillés afin prévenir les activités de blanchiment d'argent et de financement du terrorisme.

Le rapport Moneyval (2023)⁵² souligne que certains pays ont mis en place des contrôles ciblés pour limiter les abus liés aux crypto-actifs dans les jeux d'argent. Ces mesures incluent par exemple :

- Limiter les types de crypto-actifs acceptés : seuls certains peuvent être utilisés pour les dépôts ou retraits ;
- Exiger une correspondance entre les dépôts et les retraits : pour éviter les transferts complexes entre différentes monnaies numériques ;
- Fixer des plafonds de transaction : afin de réduire les montants pouvant être blanchis en une seule fois ;
- Utiliser des outils de surveillance blockchain : pour repérer des signaux à risque comme l'usage de mélangeurs (pour brouiller l'origine des fonds), de chaînes privées⁵³, ou des transferts complexes.

Toutefois, les caractéristiques mêmes des crypto-monnaies (anonymat, décentralisation) entrent en contradiction avec les normes du secteur des paris, qui exigent une identification claire des utilisateurs.

Cela pose deux grands défis aux autorités :

- Surveiller efficacement les paris légaux malgré la masse des opérateurs et des transactions ;
- Lutter contre les paris illégaux, où les opérateurs offshore ou non déclarés attirent les joueurs par des cotes plus avantageuses, moins de limites, et surtout, l'anonymat offert par les crypto-monnaies.

6. Trop peu d'enquêtes et de poursuites

Selon le rapport annuel 2022 de MONEYVAL (2023a)⁵⁴, les condamnations pour blanchiment de capitaux demeurent peu fréquentes. En outre, les enquêtes financières parallèles ne sont pas encore menées de manière systématique dans de nombreuses juridictions.

C'est également le cas dans le secteur des paris, où le nombre d'affaires aboutissant à des poursuites reste limité.

Des observations recueillies dans certaines juridictions font état d'un manque de ressources humaines et d'expertise spécialisée au sein des équipes d'enquête. La lutte contre le blanchiment via les paris en ligne nécessite des outils d'analyse avancés et des formations ciblées, qui ne sont pas encore disponibles partout.

Deux facteurs clés entravent la détection :

- L'absence de victimes identifiables, qui rend les affaires moins visibles et moins susceptibles d'être prioritaires ;
- La dimension transfrontalière de nombreuses opérations, qui complique la coopération internationale.

⁵¹ GAFI (2021). Actifs virtuels et prestataires de services d'actifs virtuels (disponible [ici](#)).

⁵² Moneyval (2023b), Risques de blanchiment d'argent et de financement du terrorisme dans le monde des actifs virtuels (disponible [ici](#)).

⁵³ Chaînes privées : blockchains dont l'accès est restreint à un groupe d'utilisateurs autorisés. Contrairement aux blockchains publiques comme Bitcoin ou Ethereum, elles ne permettent pas à tout le monde de consulter ou valider les transactions, ce qui limite la transparence et complique la traçabilité des flux financiers.

⁵⁴ Moneyval (2023a); Rapport annuel 2022 (available [here](#)).

Le manque de collaboration structurée entre les autorités de supervision et les services répressifs entre juridictions affaiblit encore l'efficacité des réponses (Commission européenne, 2024)⁵⁵. Cette fragmentation limite la capacité globale à identifier, retracer et démanteler les réseaux criminels impliqués dans le blanchiment via les paris sportifs.

CONCLUSION

1. Renforcement des mesures nationales de prévention et de détection

- Assurer la mise en œuvre effective de la directive européenne anti-blanchiment dans le secteur des paris (voir les mesures à l'Annexe 3). Les autorités nationales devraient notamment obliger les opérateurs à :
 - ✓ Elaborer une analyse des risques commerciaux cohérente et rationnelle ;
 - ✓ Vérifier l'identité des clients via une source indépendante fiable, en réduisant l'anonymat permis par certains moyens de paiement (crypto-actifs, cartes prépayées, Bitcard Secure BTC⁵⁶, etc.) ;
 - ✓ Enregistrer les données des clients pour toute transaction ou gain supérieur à 2 000 euros ;
 - ✓ Appliquer des procédures renforcées aux parieurs considérés comme à risque élevé ;
 - ✓ Verser les gains uniquement sur le compte d'origine du dépôt pour éviter les superpositions de fonds et faciliter les enquêtes.
 - ✓ Désigner un responsable référent pour les questions liées au blanchiment d'argent ;
 - ✓ Renforcer la transparence sur l'identité des actionnaires et des membres du conseil d'administration des opérateurs agréés.
- Adapter l'offre légale de paris en fonction des risques identifiés (ex. : types de paris, taux de retour aux joueurs) en s'appuyant sur une évaluation fondée sur les risques.
- Définir des critères clairs de déclaration d'activités suspectes, en collaboration avec les autorités compétentes (CRF, police, régulateurs, opérateurs)⁵⁷.

Ces critères pourraient inclure :

- ✓ Utilisation de multiples comptes ou moyens de paiement par un même individu ;
 - ✓ Origine géographique suspecte d'une carte de paiement ;
 - ✓ Fréquence inhabituelle de dépôts, retraits ou paris ;
 - ✓ Gains élevés, réguliers ou multipliés chez un même client, en particulier à cotes faibles.
- Aider les opérateurs à configurer leurs systèmes informatiques pour détecter automatiquement ces comportements suspects.
 - Donner aux autorités de régulation un accès complet aux données de paris en ligne pour mieux détecter les activités à risque.
 - Contrôler régulièrement la conformité des opérateurs avec les exigences réglementaires en matière de lutte contre le blanchiment.

⁵⁵ Conseil de l'Union européenne (2024), *Document de travail des services de la Commission accompagnant le rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre de la directive (UE) 2015/849* (disponible [ici](#)).

⁵⁶ Bitcard Secure BTC : carte prépayée permettant d'utiliser des bitcoins pour effectuer des paiements ou retirer des espèces. Ce type de solution, souvent adossé à une plateforme crypto, permet de dépenser des actifs numériques de manière relativement anonyme, ce qui en fait un vecteur potentiel de blanchiment s'il n'est pas encadré par des obligations de vérification d'identité.

⁵⁷ Conseil de l'Union européenne (2024), Proposition de règlement du parlement européen et du conseil relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (disponible [ici](#)).

- Favoriser la coopération entre autorités de régulation et secteur bancaire, notamment par des échanges encadrés d'informations pertinentes dans le respect du RGPD⁵⁸. Les banques disposent de données précieuses pour établir des profils de risque.
- Associer les intermédiaires financiers à la mise en œuvre des mesures anti-blanchiment dans le secteur des paris.

⁵⁸ RGPD : Règlement général sur la protection des données (UE 2016/679), entré en vigueur en 2018. Il encadre le traitement des données à caractère personnel au sein de l'Union européenne et garantit les droits des personnes en matière de vie privée, y compris dans les secteurs régulés comme les jeux d'argent.

2. Importance d'une coopération internationale pour améliorer les dispositifs

- Encourager la coopération entre les cellules de renseignement financier (CRF/FIU)⁵⁹ sur les questions liées aux paris et jeux d'argent, notamment par la création d'un groupe de travail dédié.
- Renforcer la collaboration et l'expertise entre les autorités nationales de régulation des paris sur le blanchiment d'argent, via des échanges de bonnes pratiques et des formations ciblées.
- Intégrer le blanchiment d'argent lié aux paris (prévention, détection, enquête, sanction) dans les travaux du Réseau des magistrats et procureurs responsables du sport (MARS), placé sous l'autorité de l'APES (Conseil de l'Europe).
- Promouvoir la mise en œuvre de mesures de recouvrement des avoirs en lien avec la manipulation des compétitions sportives.
- Lancer une étude approfondie sur le blanchiment d'argent par le vecteur des paris, comprenant trois volets :
 - ✓ Évaluation des risques, selon les trois étapes du modèle GAFI (2013)⁶⁰ : identification (menaces et vulnérabilités), analyse (nature, sources, fréquence, conséquences), évaluation (priorités et stratégies) ;
 - ✓ Typologie des systèmes de blanchiment via les paris, avec des exemples concrets, construite à partir de consultations avec le réseau MARS et d'autres parties prenantes ;
 - ✓ Analyse des liens entre le blanchiment via les paris, le blanchiment via des structures sportives, et la manipulation de compétitions.
- Sur la base de ces travaux, envisager l'adoption par le Conseil de l'Europe d'une recommandation spécifique sur la prévention, la détection et la sanction du blanchiment d'argent dans les paris.

⁵⁹ CRF (Cellule de renseignement financier) / FIU (Financial Intelligence Unit) : organisme national chargé de recevoir, d'analyser et de transmettre les déclarations d'activités suspectes en matière de blanchiment de capitaux ou de financement du terrorisme aux autorités compétentes. Chaque pays en possède une, souvent rattachée à une autorité publique.

⁶⁰ GAFI (2013), directives du GAFI. Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme (disponible [ici](#)).

ANNEXE 1 : EVALUATION DES RISQUES POUR LES MARCHES PHYSIQUES

L'évaluation des risques de la GB Gambling Commission⁶¹ porte sur le marché britannique, mais elle offre un aperçu utile de la façon dont ces risques peuvent se manifester dans d'autres contextes.

Vulnérabilité	Risque	Probabilité d'occurrence de l'événement	Impact de l'événement	Risque global
Contrôle de l'opérateur	Les opérateurs ne se conforment pas à la législation/aux règles de prévention de la lutte contre le blanchiment d'argent	Élevé	Élevé	Élevé
Contrôle de l'opérateur	Manque d'interaction efficace avec les clients, entraînant une incapacité à prévenir ou détecter le blanchiment d'argent	Moyen	Élevé	Élevé
Contrôle de l'opérateur	Insuffisance/absence de contrôles KYC entraînant le blanchiment des produits du crime par les criminels	Élevé	Élevé	Élevé
Contrôle de l'opérateur	Relations d'affaires avec des tiers et investisseurs commerciaux	Moyen	Élevé	Élevé
Octroi de licences et intégrité	Les opérations de paris sont acquises par des criminels organisés pour blanchir des fonds d'origine criminelle.	Faible	Élevé	Moyen
Octroi de licences et intégrité	Employés de sociétés de paris agissant en collusion avec des criminels organisés pour blanchir des fonds d'origine criminelle	Moyen	Élevé	Élevé
Client	Clients non vérifiés blanchissant des produits du crime par le biais de paris	Élevé	Élevé	Élevé
Client	Identification fausse ou volée utilisée pour contourner les contrôles afin de blanchir des fonds d'origine criminelle	Moyen	Élevé	Élevé
Client	Accessibilité à plusieurs locaux/exploitants	Élevé	Élevé	Élevé
Client	Les bandes criminelles organisées	Faible	Élevé	Moyen
Moyens de paiement	Transactions en espèces	Élevé	Élevé	Élevé
Moyens de paiement	Transactions sans numéraire	Moyen	Élevé	Élevé
Moyens de paiement	Notes teintées	Faible	Moyen	Faible
Moyens de paiement	Absence de système de contrôle en boucle fermée	Moyen	Élevé	Élevé
Moyens de paiement	Modes de paiement multiples	Moyen	Élevé	Élevé
Produit	Terminaux de paris en libre-service et distributeurs de billets (Ticket-in-Ticket Out) utilisés pour blanchir des fonds d'origine criminelle	Moyen	Élevé	Élevé
Produit	Apportez votre propre appareil (BYOD)	Faible	Moyen	Faible

⁶¹ Adapté de la GB Gambling Commission Risk-Assessment (2023) (disponible [ici](#)).

ANNEXE 2 : EVALUATION DES RISQUES POUR LES PLATEFORMES EN LIGNE

L'évaluation des risques de la GB Gambling Commission⁶² porte sur le marché britannique, mais elle offre un aperçu utile de la façon dont ces risques peuvent se manifester dans d'autres contextes.

Vulnérabilité	Risque	Probabilité d'occurrence de l'événement	Impact de l'événement	Risque global
Contrôle de l'opérateur	Les opérateurs ne se conforment pas à la législation/aux règles de prévention de la lutte contre le blanchiment d'argent	Élevé	Élevé	Élevé
Contrôle de l'opérateur	Les opérateurs misent et gagnent directement et indirectement sur leurs propres produits	Faible	Moyen	Faible
Contrôle de l'opérateur	le manque de compétences du personnel clé et des titulaires de licences, qui peut alors être exploité par des criminels cherchant à blanchir les produits du crime	Moyen	Élevé	Élevé
Contrôle de l'opérateur	Insuffisance/absence de contrôles KYC entraînant le blanchiment des produits du crime par les criminels	Élevé	Élevé	Élevé
Contrôle de l'opérateur	"Programmes pour les clients à forte valeur ajoutée (comptes VIP)	Moyen	Élevé	Élevé
Contrôle de l'opérateur	Seuil monétaire élevé	Élevé	Élevé	Élevé
Contrôle de l'opérateur	KYC complété au point de retrait	Moyen	Élevé	Élevé
Contrôle de l'opérateur	Relations d'affaires avec des tiers et investisseurs commerciaux	Moyen	Élevé	Élevé
Octroi de licences et intégrité	Opérations de jeu gérées ou acquises par des criminels organisés pour blanchir des fonds d'origine criminelle	Faible	Élevé	Moyen
Client	Identification fausse ou volée utilisée pour contourner les contrôles afin de blanchir des fonds d'origine criminelle	Élevé	Élevé	Élevé
Client	Accès à plusieurs comptes à distance	Moyen	Élevé	Élevé
Client	Clients issus de juridictions à Élevé risque ou non coopératives utilisant des installations à distance pour blanchir des fonds d'origine criminelle	Moyen	Élevé	Élevé
Client	"Schtroumpf"	Élevé	Élevé	Élevé
Client	"Comptes de paris "mules	Élevé	Élevé	Élevé
Client	Personnes politiquement exposées (PPE)	Moyen	Élevé	Élevé
Client	Clients d'affaires (bourse de paris)	Moyen	Élevé	Élevé
Client	Recours à des tiers ou à des agents pour dissimuler la source ou la propriété des fonds misés par les clients ainsi que leur identité.	Élevé	Élevé	Élevé
Moyens de paiement	Portefeuilles électroniques	Élevé	Moyen	Moyen
Moyens de paiement	Transactions de crypto-monnaies	Moyen	Élevé	Élevé
Moyens de paiement	Cartes prépayées	Élevé	Élevé	Élevé
Moyens de paiement	Absence de système de contrôle en boucle fermée	Moyen	Élevé	Élevé
Moyens de paiement	Modes de paiement multiples	Élevé	Élevé	Élevé
Produit	Les paris de pair à pair	Élevé	Élevé	Élevé
Produit	Événements de paris non réglementés	Moyen	Élevé	Élevé

⁶² GB Gambling Commission. (2023), Les risques de blanchiment d'argent et de financement du terrorisme dans l'industrie du jeu britannique) (disponible [ici](#)).

ANNEXE 3 : MESURES EN LIEN AVEC LA 6E DIRECTIVE EUROPEENNE ANTI-BLANCHIMENT

- **Approche fondée sur les risques** : Les entités doivent évaluer les risques de blanchiment de capitaux et de financement du terrorisme, et adapter leurs mesures de gestion et de prévention en fonction du niveau de risque identifié.
- **Connaissance du client (Know Your Customer – KYC)** : processus initial par lequel un opérateur vérifie l'identité d'un client et ses informations de base avant d'entrer en relation d'affaires. Le KYC vise principalement à confirmer les documents d'identité et à s'assurer que le client est bien la personne qu'il prétend être.
- **Vigilance à l'égard de la clientèle (Customer Due Diligence – CDD)** : processus plus large, fondé sur les risques, qui inclut l'identification KYC mais exige également d'évaluer le profil de risque du client, de comprendre l'objet et la nature de la relation, d'examiner l'origine des fonds lorsque cela est pertinent, et d'assurer une surveillance continue des opérations afin de détecter tout comportement inhabituel ou suspect.
- **Connaissance du client (KYC)** : Elles doivent vérifier l'identité des clients, comprendre la nature de la relation d'affaires et assurer un suivi continu des transactions.
- **Mesures de vigilance renforcée (EDD)** : Pour les clients ou opérations à risque élevé, des vérifications plus poussées sont requises, notamment sur leur environnement et leur surface financière apparente.
- **Personnes politiquement exposées (PPE)** : Des mesures complémentaires s'appliquent aux relations d'affaires avec des personnes exerçant une fonction publique ou celles ayant des liens étroits avec elles.
- **Transparence de la propriété effective** : Les entités doivent identifier et vérifier les bénéficiaires effectifs (personnes physiques qui contrôlent ou profitent d'une société, d'un trust, etc.).
- **Signalement des activités suspectes** : Toute activité ou transaction jugée suspecte doit être signalée sans délai aux autorités compétentes.
- **Tenue de registres** : Les entités sont tenues de conserver les documents et informations pertinents pendant toute la relation d'affaires et au-delà selon une période définie, afin de faciliter les contrôles et les enquêtes.
- **Autorités nationales de surveillance** : Chaque État membre doit disposer d'autorités chargées de faire appliquer la législation anti-blanchiment, en coordination avec les autres pays de l'UE.
- **Formation du personnel** : Les entités doivent former leurs employés à détecter les signaux d'alerte et à réagir de manière appropriée face à des comportements suspects.