ctif cfi

Cellule de Traitement des Informations Financières

RAPPORT D'ACTIVITÉS 2025

Cellule de Traitement des Informations Financières

Rapport d'activités

2025

EXECUTIVE SUMMARY

L'activité de la CTIF en quelques mots et chiffres

La CTIF a pour mission de recevoir des déclarations d'opérations, de fonds ou de faits suspects des entités assujetties à la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces[1], de ses homologues étrangers dans le cadre de la coopération internationale et d'autres services de l'Etat désignés explicitement dans la loi.

En 2025, la CTIF a reçu un total de **102.312 communications** (déclarations d'opérations, de fonds ou de faits suspects, informations des homologues étrangers et services de l'Etat – 91.487 communications reçues en 2024).

L'augmentation du nombre total de déclarations reçues est principalement due à la forte croissance observée dans le secteur des établissements de paiement avec près de 52.000 déclarations émanant en 2025 de ce secteur, soit une augmentation de près de 10.000 déclarations en une année. Néanmoins, cette hausse de l'activité déclarative doit être correctement interprétée étant donné que certains de ces établissements proposent leurs services de paiement depuis la Belgique à des clients dans plusieurs pays de l'UE, grâce au passeport européen. Plus de 90% de ces déclarations sont, après un examen par la CTIF, externalisées vers ses homologues européens dans le cadre du processus « *cross border reporting* » vu l'absence de lien direct avec notre pays.

Au cours de cette même période, la CTIF a transmis **1.334 nouveaux dossiers** aux autorités judiciaires pour un montant total de **2,13 milliards EUR** et plus de mille cinq cents informations utiles ont été communiquées aux services administratifs de l'Etat (CAF, SIRS, SPF Economie, …) et aux autorités de supervision, en application des articles 83 et 121 de la loi du 18 septembre 2017.

Si de nouvelles déclarations de soupçon sont adressées à la CTIF concernant des transactions en rapport avec la même affaire (déclarations complémentaires) et si des indices sérieux de blanchiment de capitaux ou de financement du terrorisme sont toujours présents, la CTIF communique sous forme de rapport complémentaire les nouvelles opérations suspectes.

En 2025, des informations provenant de 2.736 déclarations de soupçon et communications reçues par la CTIF ont été utilisées dans le cadre de transmissions de dossiers aux autorités judiciaires, indépendamment des autres mécanismes de dissémination de l'information aux niveaux national et international.

En l'absence d'indices sérieux de blanchiment ou de financement du terrorisme, la CTIF n'effectue aucune communication aux autorités judiciaires, mais les informations issues des déclarations de soupçon ne sont pas perdues pour autant.

Même si un dossier n'est pas transmis aux autorités judiciaires, les informations qu'il contient peuvent être transmises par la CTIF aux services de renseignements et à l'OCAM dans le cadre de la lutte contre le processus de radicalisation, le terrorisme, son financement et les activités de blanchiment qui pourraient y être liées.

Cette année encore, la CTIF a adressé de nombreuses demandes de renseignements à l'étranger et en a également reçu un grand nombre de la part de ses **homologues** de pays européens ou de pays tiers.

[1] Ci-après la loi du 18 septembre 2017. Moniteur belge du 6 octobre 2017 - Chambre des représentants (www.lachambre.be) Documents : 54-2566.

Temps forts de l'année 2025

L'année 2025 marque également la publication du **rapport d'évaluation mutuelle de la Belgique par le GAFI**[2]. Cette évaluation analyse en profondeur la mise en œuvre et l'efficacité des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive en Belgique. Une description du système belge LBC/FT[3], ainsi que des recommandations ciblées pour le renforcer davantage, figurent dans ce rapport. Etant donné le rôle central de la CTIF dans le système LBC/FT, les évaluateurs se sont également penchés sur plusieurs aspects fondamentaux liés aux renseignements financiers. La Belgique est notée comme ayant un niveau d'efficacité significatif dans ce domaine.

Par ailleurs, dans le cadre du retour sectoriel destiné aux déclarants, un nouveau format d'**Ateliers LBC/FT** a vu le jour, dont deux éditions ont été organisées par la CTIF en 2025. Une première édition, proposée aux professions financières, a été consacrée au thème de la corruption, en abordant l'aspect LBC préventif mais aussi répressif, couvrant ainsi le cycle de vie de la déclaration, allant du moindre soupçon, vers l'analyse et les potentiels indices sérieux de BC, et terminant en une potentielle enquête au Parquet. Le second Atelier s'est orienté vers les professions non financières, en réunissant le secteur des professions comptables et fiscales, où les discussions ont notamment porté sur la protection du déclarant, l'utilité de la déclaration dans le système LBC/FT, les typologies et risques rencontrés par le secteur ou encore la qualité des informations fournies sur goAML.

Alors que 2024 était encore consacré à des travaux préparatoires concernant les locaux de l'**AMLA** à Francfort et le recrutement de personnel, nous avons observé en 2025 que l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme a pris des mesures plus concrètes en matière de coordination et de soutien des CRF de l'UE. Nous pouvons affirmer que l'AMLA a déjà réalisé de nombreux progrès en peu de temps, que l'intégration de tous les délégués des CRF est essentielle pour diffuser et renforcer la connaissance du monde des CRF au sein de l'AMLA, et que le rôle des CRF est de continuer à veiller au respect de leur autonomie et de leur indépendance en recherchant des solutions flexibles et coordonnées.

Tendances en matière de blanchiment de capitaux et financement du terrorisme

Au cours des dernières années, le paysage financier a connu une évolution significative. Sous l'influence de l'innovation technologique, une transformation s'est réalisée en l'espace d'une décennie, passant d'un environnement fondé sur la banque traditionnelle à un écosystème financier numérique, orienté vers les données. Cette évolution irréversible est portée par un secteur fintech en plein essor, tant en Belgique qu'en Europe, et présente de nombreux avantages pour les consommateurs. L'Union européenne (UE) s'engage résolument en faveur de cette transformation numérique du secteur financier tout en essayant d'apporter des ajustements dans un certain nombre de domaines. Plusieurs initiatives législatives de l'UE sont de ce fait entrées (partiellement) en vigueur en 2025, telles que le règlement sur les « paiements instantanés » (IPR)[4] et le règlement relatif aux « crypto-actifs » (MICAR)[5].

Comme c'est souvent le cas, les organisations criminelles se révèlent également être « précurseurs » en matière de blanchiment de capitaux et de financement du terrorisme lorsqu'il s'agit d'utiliser les nouvelles technologies. Toutes criminalités confondues, la CTIF a observé que **l'utilisation de la technologie** dans les montages de blanchiment constituait le fil conducteur en 2025. Ainsi, les organisations criminelles

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Evaluation-mutuelle-Belgique-2025.pdf.coredownload.inline.pdf

[3] LBC/FT : Lutte contre le blanchiment de capitaux et le financement du terrorisme

[4] EU 2024/886

[5] EU 2023/114

exploitent pleinement la rapidité accrue – lors de l'ouverture de comptes en ligne et de l'exécution de transactions transfrontalières – offerte tant par les banques traditionnelles que par les nouveaux prestataires de services de paiements (PSP). On observe également de fréquents changements d'actifs, avec une transition fluide de la monnaie scripturale vers les actifs virtuels et vice versa. L'association ou l'intégration des PSP et des prestataires de services d'actifs virtuels (*Virtual Asset Service Providers* ou *VASP*) facilite cette conversion et complexifie le suivi de la piste financière par les services d'enquête.

Les criminels associent de manière quelque peu paradoxale l'usage de la technologie financière au sens large à **des techniques traditionnelles** pour mettre en place des schémas de blanchiment. Il apparaît ainsi qu'indépendamment de l'infraction sous-jacente, les espèces continuent de jouer un rôle crucial dans le transfert de valeur et la dissimulation de l'origine des fonds. L'or pourrait également faire un retour significatif dans les montages de blanchiment de capitaux, en raison de la forte hausse de son cours pendant l'année 2025. Dans les dossiers les plus complexes, les technologies financières modernes sont combinées adéquatement à l'utilisation du cash. Les réseaux professionnels de blanchiment de capitaux – qui, comme lors des années précédentes, peuvent être considérés comme la principale tendance et menace en matière de blanchiment – disposent d'un grand nombre de comptes en ligne ouverts auprès d'établissements de paiement, tout en continuant à gérer des liquidités provenant notamment du trafic de stupéfiants via le paiement de travail au noir. Cette synergie entre l'évolution des technologies financières et l'utilisation des méthodes traditionnelles se reflète tant dans l'analyse des menaces criminelles que dans les techniques employées pour le blanchiment de capitaux et le financement du terrorisme.

La menace terroriste est restée élevée en 2025. Bien qu'elle soit complexe et provienne de différentes sources, les partenaires de renseignement et de sécurité ont identifié que la principale menace émane de petites cellules et d'acteurs isolés inspirés par l'idéologie de l'État islamique[6]. Ce constat se reflète également dans les dossiers relatifs au financement du terrorisme transmis par la CTIF aux parquets, où le djihadisme islamique demeure prédominant.

Bien que la combinaison de nouvelles possibilités techniques et de méthodes éprouvées se révèle très efficace et pose des défis considérables aux services d'enquête financière, elle peut aussi constituer une source d'inspiration. En effet, en matière de lutte contre le blanchiment et la détection des opérations suspectes, on recherche également un modèle fondé sur les données. L'intégration de méthodes anciennes et modernes n'est pas uniquement constatée dans le processus de blanchiment mais peut également être mise en œuvre comme stratégie de lutte contre ce phénomène.

[6] VSSE (2025) Intelligence Rapport

TABLE DES MATIERES

I. AVANT-PROPOS DU PRESIDENT DE LA CELLULE DE TRAITEMENT DES INFORMATIONS FINANCIERES

Comme chaque année, le nouveau rapport d'activité de la CTIF m'amène à satisfaire à une obligation qui n'est pas une formule de politesse ou de courtoisie : il m'est particulièrement agréable de remercier l'ensemble des collaborateurs de la Cellule pour l'intense travail accompli. Les statistiques que je commenterai ne reflètent que le produit fini de l'activité de la CTIF sans prendre en compte toutes les autres tâches logistiques et administratives quotidiennes assumées.

Je tiens à remercier également tous nos partenaires extérieurs impliqués à quelque titre que ce soit dans la lutte contre le blanchiment d'argent et le financement du terrorisme. Les contacts noués tant avec les collègues du monde judiciaire, avec la Policé fédérale, les Services de renseignement, les départements administratifs de l'Etat qu'avec les partenaires privés renforcent l'action de la CTIF.

Quelques mots à propos des statistiques de l'année 2025 :

En introduction du rapport 2024, j'écrivais qu'il est de coutume de dire que les chiffres parlent d'eux-mêmes.

Aujourd'hui, les chiffres surprennent et interpellent.

102.312 communications reçues en 2025, 1.334 nouveaux dossiers aux autorités judiciaires pour un montant total de 2,13 milliards EUR et plus de mille cinq cents informations utiles ont été communiquées aux services administratifs de l'Etat (CAF, SIRS, SPF Economie, …) et aux autorités de supervision.

L'augmentation constante du nombre de communications reflète l'implication des entités assujetties dans la lutte contre les phénomènes de blanchiment même lorsque les opérations ne se déroulent pas exclusivement en Belgique.

Les blanchisseurs d'argent sale débordent d'imagination pour parvenir à leurs fins et recourent à des mécanismes à la complexité variable présentant néanmoins des constantes de fiabilité et de coût.

Le mot d'ordre des blanchisseurs professionnels, c'est trouver le moyen de blanchir le plus sûr et le moins cher !

Dans ce rapport, le rôle clef joué par des blanchisseurs professionnels est mis en évidence, rôle également souligné lors de la récente conférence de l'AMLA[7]. Ces « courtiers » criminels jouent tantôt le rôle de banquier informel, de convoyeur de fonds ou de logisticien en proposant des structures commerciales émettant des documents nécessaires pour camoufler les opérations de blanchiment.

Prendre la correcte mesure du rôle des blanchisseurs professionnels constitue un préalable à une lutte efficace.

Aujourd'hui, cela ne suppose plus nécessairement et obligatoirement, une complexification de la législation anti-blanchiment qui ne viserait que les acteurs régulables[8]. Ainsi, il semble nécessaire de s'intéresser à la question de la dissolution rapide de sociétés commerciales qui apparaissent comme des coquilles vides et constituent des instruments faciles pour les blanchisseurs professionnels.

[7] Javier Zarzalejos, député au Parlement européen et président de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE), 9 juin 2026.
[8] La formule est empruntée à Quentin Mugg, voir son article intitulé « Comment mieux lutter contre les courtiers criminels, ces moteurs invisibles du blanchiment d'argent », Le nouvel Observateur, 13 novembre 2025.

À cet égard, la problématique des « coquilles vides » est régulièrement soulignée au niveau international. Le récent rapport d'évaluation mutuelle de la Belgique par le GAFI[9] indique ainsi que les mesures actuelles d'atténuation des risques liés aux personnes morales demeurent limitées et que les autorités procèdent de manière soutenue à la radiation et à la dissolution d'entités inactives afin de limiter leur usage abusif.

Quoi qu'il en soit, il est impératif de poursuivre, de renforcer, d'intensifier le dialogue ou le partenariat entre autorités publiques. L'intensification de la lutte et la récupération des avoirs criminels reposent finalement sur la devise de notre pays... L'Union fait la force !

Je vous souhaite une agréable lecture.

Philippe de KOSTER
Président de la CTIF

[9] https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Evaluation-mutuelle-Belgique-2025.pdf.coredownload.inline.pdf

II. COMPOSITION DE LA CTIF

Président :	M.	Philippe de KOSTER
Vice-président :	M.	Fons BORGINON
Présidents suppléants :	MM.	Christophe REINESON Bart VAN HULST
Membres :	MM.	Geoffrey DELRÉE Philippe GARZANITI Jean-François VANDERMEULEN Benoit WOLTER
Secrétaire général :	M.	Kris MESKENS

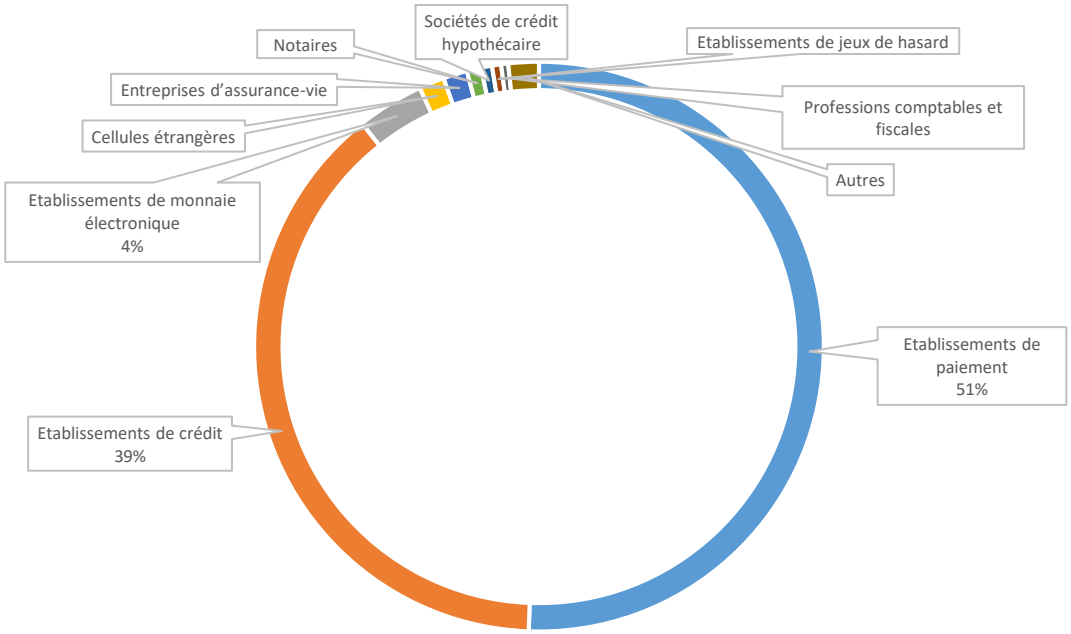
III. L'ANNEE 2025 EN QUELQUES CHIFFRES

La CTIF a pour mission de recevoir des déclarations d'opérations, de fonds ou de faits suspects des entités assujetties à la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces[10], et des informations de ses homologues étrangers dans le cadre de la coopération internationale et d'autres services de l'Etat désignés explicitement dans la loi.

En 2025, la CTIF a reçu un total de **102.312 communications** (déclarations d'opérations, de fonds ou de faits suspects, et informations des homologues étrangers et services de l'Etat).

	2023	2024	2025
Nombre total de communications reçues	79.211	91.487	102.312

L'essentiel des déclarations de soupçon proviennent des établissements de paiement et des établissements de crédit.



[10] Ci-après la loi du 18 septembre 2017. Moniteur belge du 6 octobre 2017 - Chambre des représentants (www.lachambre.be) Documents : 54-2566.

Le contenu d'une partie importante des déclarations de soupçon, essentiellement reçues d'établissements de paiement agréés en Belgique pour des activités exercées dans l'Union Européenne en libre prestation de services, est externalisé vers les homologues européens de la CTIF (échanges automatiques, spontanés et à la demande)[11].

Les autres déclarations et informations reçues sont analysées et enrichies, et le cas échéant, la CTIF transmet le résultat de son analyse aux autorités judiciaires, lorsqu'il existe des indices sérieux de blanchiment ou de financement du terrorisme ou de financement de la prolifération des armes de destruction massives. En 2025, la CTIF a transmis **1.334 nouveaux dossiers** aux autorités judiciaires pour un montant total de **2,13 milliards EUR.**

La CTIF partage également comme prévu par la loi des informations spécifiques avec plusieurs autorités compétentes[12] au niveau national, avec les services de renseignement civil et militaire, avec l'OCAM et avec les autorités de supervision des entités assujetties.

La CTIF avise par ailleurs l'Organe Central pour la Saisie et la Confiscation (OCSC) lorsque des avoirs d'une valeur significative, de quelque nature qu'ils soient, sont disponibles en vue d'une éventuelle saisie judiciaire[13].

Les informations reçues qui ne peuvent pas être externalisées par la CTIF ne sont pas perdues pour autant car elles constituent un socle essentiel d'informations, disponibles à des fins d'analyse stratégique mais aussi pour une analyse ultérieure par la division opérationnelle au cas où de nouvelles informations pertinentes (nouvelles informations financières, renseignements policiers, nouvelles enquêtes judiciaires,…) permettraient de les mettre en relation avec du blanchiment de capitaux ou du financement du terrorisme.

Un aperçu détaillé des statistiques 2025 est repris au point V.

[11] Voir page 47 pour plus de détails.
[12] Notamment le Service de Coordination Anti-Fraude du SPF Finances (CAF) lorsque la transmission au procureur concerne des informations relatives au blanchiment de capitaux provenant de la commission d'une infraction pouvant avoir des répercussions en matière de fraude fiscale grave, l'Administration Générale des Douanes et Accises lorsque la transmission au procureur concerne des informations relatives au blanchiment de capitaux provenant d'infractions pour lesquelles l'Administration Générale des Douanes et Accises exerce l'action publique, les autorités de contrôle des entités assujetties lorsque la transmission au procureur concerne des informations relatives au blanchiment de capitaux provenant d'infractions pour lesquelles ces autorités possèdent une compétence d'enquête et/ou de contrôle, le Service d'Information et de Recherche Sociale (SIRS) lorsque la transmission au procureur concerne des informations relatives au blanchiment de capitaux provenant de la commission d'une infraction pouvant avoir des répercussions en matière de fraude sociale, l'auditeur du travail lorsque la transmission au procureur concerne des informations relatives au blanchiment de capitaux provenant du trafic d'êtres humains, de la traite des êtres humains ou de la fraude sociale et l'Administration Générale de la Trésorerie lorsque la CTIF dispose d'informations utiles pour cette autorité en matière de gel des avoirs ou de contrôle du respect des mesures d'embargos.
[13] Voir page 38 pour plus de détails.

IV. TENDANCES DU BLANCHIMENT DE CAPITAUX ET DU FINANCEMENT DU TERRORISME

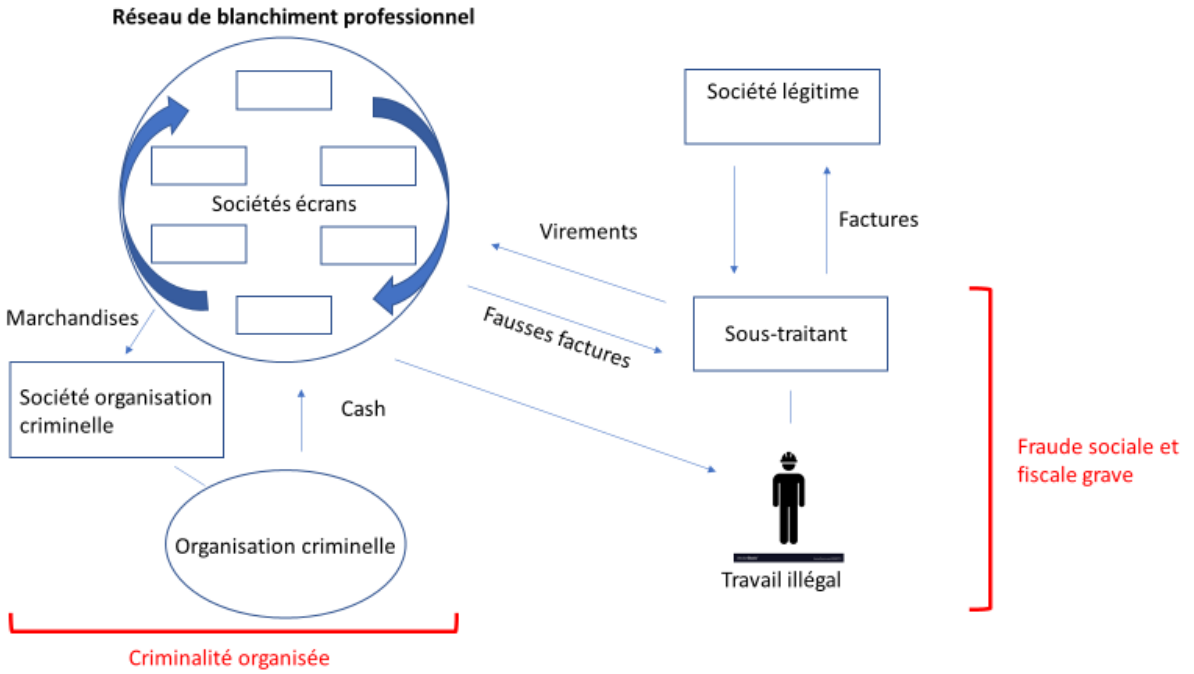
1. Tendances en matière de blanchiment de capitaux

1.1. Principales menaces criminelles

1.1.1. Réseaux professionnels de blanchiment

Dans le cadre de l'analyse des dossiers liés à la criminalité organisée, la CTIF utilise la définition criminologique du terme, tandis que le droit pénal utilise la notion d'« organisation criminelle ». Le type de dossiers que la CTIF considère comme relevant de la criminalité organisée est varié et cette qualification est relativement subjective étant donné que les dossiers complexes peuvent contenir des éléments de plusieurs autres infractions sous-jacentes. Tel est le cas des dossiers relatifs **aux réseaux professionnels de blanchiment** qui constituent, cette année encore, la principale tendance en matière de blanchiment et concernent la majorité des dossiers liés à la criminalité organisée.

Représentation schématique d'un réseau professionnel de blanchiment et de ses différents aspects criminels



Les réseaux professionnels de blanchiment offrent leur service à différentes organisations criminelles et ne sont généralement pas impliqués dans les activités criminelles qui génèrent ces fonds. Ils disposent d'un réseau international de **sociétés écrans** et de **mules financières**, dont les comptes sont utilisés pour faire circuler d'importantes sommes d'argent. Grâce à la technique de **la compensation**, la valeur est transférée et l'argent liquide peut être utilisé pour rémunérer du travail illégal. Les capitaux illégaux sont mélangés avec des capitaux légaux en recourant à **des paiements pour compte de tiers** ou ***Third Party Payments***, de sorte que des sociétés n'appartenant pas au réseau participent, consciemment ou inconsciemment, au processus de blanchiment.

Le mélange de fonds obtenus légalement et illégalement et la combinaison d'activités légales et illégales constituent les stratégies principales des réseaux professionnels de blanchiment. Souvent,

une partie des activités est correctement facturée, les sous-traitants continuant simplement à travailler au noir en dehors du contrat officiel. Dans le commerce (de détail), également, une partie des achats et des ventes peut ne pas être enregistrée, facilitant ainsi l'intégration de fonds illicites dans le chiffre d'affaires. Le fonds de commerce et l'aménagement des commerces reposent fréquemment sur des capitaux d'origine criminelle.

Les sociétés qui exercent des activités réelles constituent la partie la plus visible du réseau de blanchiment et sont principalement utilisées pour absorber le cash du réseau. Ces sociétés effectuent à leur tour des paiements vers la partie la moins visible du réseau, composée de dizaines de sociétés fantômes ou de sociétés écrans qui émettent des fausses factures et sont gérées administrativement par des prête-noms.

Les montants qui circulent sur les comptes des sociétés écrans sont très importants, il s'agit souvent de plusieurs millions d'euros en l'espace de quelques mois.

Les fonds sont ensuite transférés à l'échelle internationale, en recourant à des paiements pour compte de tiers afin de brouiller davantage les pistes. À la fin du processus, des marchandises peuvent être achetées ou des biens immobiliers acquis à l'étranger, les véritables bénéficiaires étant les commanditaires qui ont mis l'argent noir à la disposition du réseau de blanchiment.

Lorsque des fonds d'origine criminelle sont utilisés directement pour rémunérer du travail non déclaré, ils ne laissent aucune trace dans le système financier, rendant les paiements indétectables. Le volume d'argent liquide provenant d'activités illégales telles que le trafic de stupéfiants est cependant très important. Lorsque des sommes importantes doivent être versées sur les comptes de sociétés écrans, ces dépôts en espèces peuvent se démarquer du flux des paiements habituels et engendrer une déclaration à la CTIF. De même, lors du transfert de fonds ou de l'acquisition de biens immobiliers ou de marchandises par les sociétés écrans au profit de l'organisation criminelle, le système bancaire traditionnel est utilisé, rendant le réseau vulnérable. C'est pourquoi, pour ces étapes, les réseaux de blanchisseurs professionnels recherchent des moyens alternatifs pour échapper à la détection, tels que le recours à des établissements de paiement étrangers et la conversion des fonds en cryptomonnaies.

Malgré la complexité de ces réseaux, la CTIF a pu, dans plusieurs dossiers, établir des liens avec des activités criminelles sous-jacentes. Ainsi, des paiements émanant du réseau de blanchiment ont été identifiés pour la location de biens utilisés à des fins d'exploitation de la prostitution ou des sommes provenant des victimes d'une vaste fraude via un service de *helpdesk* ont été versées sur les comptes de sociétés écrans. Dans un nombre limité de dossiers, les fonds ont pu être retracés, via des sociétés étrangères, jusqu'à des personnes déjà connues pour leur implication dans un trafic de stupéfiants à grande échelle.

La CTIF n'a toutefois pas toujours une vue d'ensemble du réseau. Si les liens avec le réseau professionnel ne peuvent être clairement démontrés, les dossiers sont transmis avec la fraude sociale et/ou la fraude fiscale grave comme infractions sous-jacentes.

1.1.2. Trafic de stupéfiants

Le marché des drogues illégales dans l'UE représenterait plus de 30 milliards d'euros[14] et constitue le principal moteur de la criminalité organisée dans les pays européens. En outre, avec le port d'Anvers, la Belgique est l'une des principales portes d'entrée de la cocaïne sud-américaine et, avec les Pays-Bas, notre pays reste une zone de production majeure de drogues de synthèse à l'échelle mondiale.

[14] *EU Drug Markets Analysis*, European Drug Agency (EUDA), Europol

Malgré ce rôle prépondérant, les profits colossaux issus du trafic international de stupéfiants ne sont certainement pas entièrement blanchis via la Belgique. Les flux commerciaux et les flux financiers suivent rarement le même trajet. Néanmoins, une part significative des fonds reste d'une manière ou d'une autre liée à notre pays. La lutte contre le blanchiment de capitaux issus du trafic de stupéfiants constitue depuis des années une priorité absolue pour la CTIF.

Les réseaux professionnels de blanchiment – dont il est question dans les dossiers liés à la criminalité organisée – assurent le blanchiment de la majeure partie des fonds issus du trafic de stupéfiants. Les dossiers qualifiés de « blanchiment issu du trafic de stupéfiants » correspondent majoritairement à du ***self laundering*** : des individus qui blanchissent eux-mêmes les revenus de leur trafic sans faire appel à un réseau externe.

La manière dont les fonds provenant du trafic de stupéfiants sont dissimulés restent globalement constants par rapport aux périodes antérieures.

À l'instar des réseaux professionnels de blanchiment, les organisations et les individus qui blanchissent eux-mêmes les revenus issus de leur trafic de stupéfiants misent pleinement sur les nouvelles technologies, tout en conservant en partie les moyens de paiement classiques.

Le trafic de stupéfiants reste fortement dépendant des espèces, en particulier au niveau des exécutants et, dans une moindre mesure, à celui des commanditaires. Dans plusieurs dossiers, la CTIF a en outre constaté des opérations sur des comptes liées au commerce de l'or, utilisé comme alternative aux espèces.

Les transactions en espèces ont également été combinées avec des paiements effectués par le biais d'établissements de paiement. Dans des points de vente physiques tels que des *nightshops* ou des commerces de détail, il est possible d'obtenir un crédit à dépenser en ligne sous la forme d'un code ou d'une carte prépayée, payable en espèces. En raison de l'augmentation de la vente de drogues en ligne, notamment via les réseaux sociaux (groupes de discussion privés) et les services de messagerie cryptée, l'utilisation des services de paiement en ligne s'est accrue, souvent via un « bouton de paiement » immédiatement accessible dans l'application même utilisée pour la vente. Pour blanchir les revenus issus de ce trafic, les mêmes services de paiement que pour la vente sont utilisés, mais cette fois-ci pour faire circuler les revenus ou les transférer à l'étranger.

Par ailleurs, certaines applications de paiement proposent, via leurs plateformes, un accès direct aux crypto-actifs et aux sites de jeux d'argent en ligne, ce qui constitue souvent la dernière étape avant que les fonds ne soient transférés sur le compte bancaire des bénéficiaires finaux du trafic de stupéfiants ou employés pour l'acquisition de biens de luxe ou de biens immobiliers.

Le parcours des revenus générés par le trafic de stupéfiants n'est cependant pas toujours aussi complexe. Le cash est souvent simplement versé directement sur des comptes. Lorsqu'il s'agit de personnes physiques, l'explication avancée est souvent qu'un prêt a été accordé à des membres de la famille ou à des amis et que cet argent a été remboursé en espèces. Dans le cas des personnes morales, les fonds provenant du trafic de stupéfiants sont mélangés à des revenus légaux en espèces. Ces sociétés exercent donc généralement des activités génératrices de liquidités et peuvent justifier le versement de sommes importantes en espèces sur leurs comptes. Parmi les exemples tirés des dossiers, on trouve notamment des sociétés actives dans le commerce de véhicules d'occasion, l'hôtellerie et la restauration, l'alimentation, le commerce de détail, les stations-service ou les produits de luxe. L'exploitation physique de ces commerces offre souvent à l'organisation criminelle, outre la possibilité de blanchir, un avantage logistique, tel que l'accès à des véhicules pour le trafic dans le cas d'un concessionnaire automobile ou à un point de vente et de collecte dans le cas de l'horeca. Enfin, les fonds d'origine criminelle ne sont pas toujours blanchis par le biais des flux de trésorerie des sociétés, mais peuvent également l'être lors de la constitution du fonds de commerce, par l'achat de machines ou l'aménagement de l'établissement.

1.1.3. Escroquerie

L'escroquerie constitue depuis plusieurs années l'une des principales infractions sous-jacentes au blanchiment de capitaux, comme en témoigne le nombre de dossiers transmis par la CTIF aux autorités judiciaires. Cette tendance se confirme en 2025. Différents services engagés dans la lutte contre l'escroquerie, tels que le SPF Économie, la police, la FSMA, Febelfin et le Centre for Cybersecurity Belgium (CCB), mettent en avant que les diverses formes d'escroquerie en ligne ont fortement augmenté au cours de l'année écoulée.

Par ailleurs, les cas révélés ne représentent que la partie visible de l'iceberg car une grande partie des victimes ne porte probablement pas plainte.

Bien que les montants en jeu dans les dossiers soient généralement relativement faibles, il s'agit néanmoins d'une menace criminelle qui engendre un important coût social et personnel et qui peut ébranler la confiance des consommateurs dans le système financier.

Les principales formes d'escroquerie en ligne observées par la CTIF dans les dossiers transmis sont le ***phishing*** et **la fraude à l'investissement**. Comme en 2024, le nombre de dossiers liés à la fraude à l'investissement demeure élevé et les montants en jeu sont en moyenne plus importants que dans les cas de *phishing*. Les montants les plus élevés ont cependant été observés dans des dossiers portant sur des schémas d'escroquerie classiques, impliquant des investissements immobiliers à l'étranger, des projets de construction, des placements (hors ligne) ou des subventions. Ce sont également ces dossiers qui justifient le montant total relativement élevé des dossiers transmis par rapport aux années antérieures.

La CTIF constate également que le blanchiment des capitaux issus de l'escroquerie est de plus en plus orchestré par des réseaux professionnels. Ainsi, il a été clairement établi, dans un dossier, que les revenus d'une fraude à grande échelle via un service de *helpdesk* avaient été transférés vers les comptes de sociétés écrans appartenant à un réseau professionnel de blanchiment qui recevait également des fonds provenant de la fraude sociale.

En outre, l'utilisation intensive de la technologie est également notable, non seulement dans le cadre de l'escroquerie elle-même, mais aussi dans le blanchiment des revenus qui en découlent. L'intelligence artificielle est utilisée pour créer des *deepfakes* de personnalités connues afin d'attirer les victimes vers des plateformes d'investissement frauduleuses, ou pour sélectionner des victimes potentielles. Des kits de *phishing* (des logiciels prêts à l'emploi permettant de mener une attaque de *phishing*) sont également disponibles sur internet, sans nécessité d'expertise technique pour mettre en place une escroquerie.

A l'instar d'autres infractions sous-jacentes, les nouvelles technologies de paiement sont détournées pour blanchir l'argent issu de l'escroquerie. Les fonds sont transférés depuis les comptes des victimes vers des établissements de paiement à l'étranger, qui servent de passerelle vers des plateformes de cryptomonnaie et des sites de paris en ligne, rendant ainsi plus complexe la traçabilité ultérieure des fonds.

1.1.4. Fraude sociale et fraude fiscale grave

La fraude sociale

La lutte contre la fraude sociale a été placée au cœur des priorités de la politique fédérale dans le cadre de l'accord de gouvernement pour la législature 2025-2029. Cette lutte s'articule autour d'un plan stratégique et d'un plan d'action opérationnel qui combinent un renforcement des contrôles et une approche axée sur les risques. L'objectif est notamment de mieux détecter et sanctionner les fraudes organisées. L'accent est également mis sur une coopération renforcée entre les services. À

cette fin, la CTIF et le Service d'Information et de Recherche Sociale (SIRS) ont intensifié leur collaboration en 2025, tant au niveau opérationnel que stratégique.

Dès 2017, la fraude sociale a été ajoutée à la liste des criminalités sous-jacentes au blanchiment. Cet ajout a permis à la CTIF de contribuer à la lutte contre ce phénomène criminel et, en particulier, de mieux appréhender ceux qui mettent en place et organisent les réseaux de fraudes tant au niveau national qu'international.

Depuis, la CTIF transmet chaque année un nombre important de dossiers aux autorités judiciaires en lien avec la fraude sociale. Loin de s'essouffler, l'examen des dossiers révèle une **amplification du phénomène** à plusieurs niveaux : le nombre de transmissions est en hausse, les montants en jeu se chiffrent en millions d'euros et de nombreuses ramifications ont pu être établies entre différents dossiers.

La fraude sociale est souvent l'aspect le plus tangible d'un réseau professionnel de blanchiment ; le travail au noir servant à blanchir des fonds provenant d'autres activités criminelles.

Des sociétés actives dans des secteurs très concurrentiels, tels que la construction, cherchent à réaliser leurs chantiers au coût le plus bas possible. Pour ce faire, elles recherchent des sous-traitants à prix réduit. Cette mise en concurrence pousse certains sous-traitants à enfreindre leurs obligations légales, notamment en matière de sécurité sociale, afin de proposer des tarifs plus compétitifs. Pour rémunérer leur main-d'œuvre non déclarée, ces sociétés ont besoin de liquidités. Afin de ne pas éveiller les soupçons des banques avec des retraits importants en espèces, elles se tournent vers des sociétés de compensation appartenant à un réseau de blanchiment professionnel.

En 2025, la CTIF a toutefois constaté une recrudescence du recours aux espèces dans le cadre de certains dossiers impliquant des ressortissants d'Europe de l'Est, ayant fondé une entreprise individuelle et servant manifestement de mules financières. Dans ces dossiers, la CTIF a observé l'ouverture de nombreux comptes exclusivement alimentés par des factures émanant de sociétés actives dans le secteur de la construction et/ou du nettoyage, dont les montants ont très rapidement fait l'objet d'importants retraits en espèces, dépassant dans plusieurs cas le million d'euros sur une période très courte.

La fraude fiscale grave

Ces dernières années, la CTIF a régulièrement été amenée à examiner des dossiers impliquant des **montages de compensation**. Outre les aspects liés à la fraude sociale, ces dossiers comportent également un volet de blanchiment lié à une fraude fiscale grave. La fraude sociale concernant des paiements non déclarés implique donc des fonds qui échappent au contrôle de l'administration fiscale. Cet aspect permet notamment de transmettre les informations pertinentes au SPF Finances par l'intermédiaire du Service de Coordination Anti-Fraude (CAF).

Outre les déclarations concernant les sociétés de compensation, la CTIF reçoit un nombre croissant de déclarations concernant des sociétés ayant une réelle activité économique dans des secteurs tels que la construction ou le nettoyage et qui recourent manifestement à des sociétés de compensation afin d'obtenir des espèces en échange de virements bancaires.

L'utilisation délibérée et répétée de **fausses factures**, notamment pour obtenir des espèces destinées à rémunérer des prestations non déclarées ou à détourner illégalement des fonds de la société,

entraîne d'importantes conséquences fiscales. Le recours à de fausses factures permet, en effet, de réduire frauduleusement le bénéfice déclaré, diminuant ainsi l'assiette fiscale de la société. Par ailleurs, le mécanisme mis en place pour rémunérer du personnel non déclaré a également un impact significatif sur l'impôt des personnes physiques.

Dans ce contexte, les méthodes employées (y compris l'utilisation de sociétés écrans) et le recours répété à la facturation fictive révèlent des indices sérieux de blanchiment de capitaux issus d'une fraude fiscale grave, permettant à la CTIF d'aviser le CAF.

Oppositions

En 2025, la CTIF a informé l'Organe Central pour la Saisie et la Confiscation (OCSC) dans un nombre particulièrement élevé de dossiers lorsque des montants ou des avoirs étaient disponibles en vue d'une saisie judiciaire. Dans le cadre d'une politique de « catch the money », la possibilité de bloquer des comptes pendant cinq jours constitue une arme importante, qui peut également être utilisée dans la lutte contre la fraude fiscale grave.

1.1.5. Autres menaces criminelles

Corruption – détournement de fonds

En 2025, la CTIF a de nouveau transmis aux autorités judiciaires plusieurs dossiers dans lesquels la corruption ou le détournement de fonds par des personnes exerçant une fonction publique ont été identifiés comme principales infractions sous-jacentes au blanchiment.

Ces dossiers concernaient des personnes présentant un risque accru de conflits d'intérêts, d'abus de fonction, de position ou d'influence, de corruption ou de criminalité financière et économique, parmi lesquelles figuraient des personnes politiquement exposées (PPE)[15], d'anciens dirigeants de ministères étrangers et d'agences de l'UE, des (anciens) collaborateurs belges d'organisations internationales et d'intercommunales, des employés portuaires nationaux et des entrepreneurs étrangers en contact étroit avec des fonctionnaires locaux.

Les opérations suspectes tendraient à indiquer à la fois la réception et le paiement de pots-de-vin, ainsi que la circulation et l'utilisation ultérieures des produits issus de **diverses formes de corruption**, y compris la corruption publique et privée, la corruption active et passive, la corruption de fonctionnaires étrangers dans le cadre de transactions commerciales internationales[16] et la corruption dans le cadre des dépenses de l'UE. Sur le plan typologique, on peut distinguer la corruption politique de haut niveau, la corruption dans les marchés publics et la corruption dans des secteurs considérés comme à risque (santé, défense, technologie, gestion des ressources naturelles, etc.).

Dans plusieurs dossiers, il était question de paiements dont le but indéniable était d'inciter des personnes exerçant une fonction publique, des dirigeants de personnes morales ou du personnel portuaire à commettre des actes illicites ou des infractions dans le cadre de l'exercice de leurs fonctions. Il s'agissait tant de paiements directs aux personnes concernées que de paiements via des tiers – des sociétés (écrans) ou des cabinets de conseil créés par d'anciennes PPE ou d'anciens collaborateurs d'organisations internationales peu après la fin de leur mandat politique ou de leur fonction – dans le cadre desquels des flux financiers illégaux étaient masqués par des communications vagues ou des fausses factures.

---

[15] La liste des fonctions considérées comme des fonctions publiques de premier plan figure à l'annexe IV de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces. Un aperçu des fonctions publiques de premier plan au niveau des organisations internationales et au niveau des institutions et organes de l'Union peut être consulté via le lien suivant (https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:C_202300724).

[16] Voir la Convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales (https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/fighting-foreign-bribery/Convention%20and%20commentaries%20booklet%202024.pdf).

Les analyses de la CTIF confirment l'utilisation d'instruments financiers bien connus pour blanchir les produits de la corruption et du détournement de fonds, ainsi que de méthodes et techniques de blanchiment largement répandues.

Des indices ont été découverts indiquant que des systèmes financiers parallèles ont été utilisés pour transférer des fonds provenant de la corruption et du détournement de fonds publics à l'étranger vers des comptes ouverts auprès d'établissements de crédit ou d'une étude notariale en Belgique.

Des publications récentes d'instances internationales et les rapports d'activité de la CTIF ont souligné que la corruption constitue un mode opératoire criminel majeur. Les éléments et circonstances relevés dans plusieurs dossiers de la CTIF ont donné lieu, en 2025, à des soupçons selon lesquels la corruption aurait facilité d'autres activités criminelles, notamment le trafic de stupéfiants, la criminalité organisée, la traite des êtres humains et la criminalité environnementale.

Ainsi, au cours de la même période, deux dockers ont changé des devises étrangères en euros dans le même bureau de change à Anvers. Tous deux ont indiqué qu'il s'agissait d'argent qu'il leur restait suite à des vacances dans un pays d'Amérique du Nord, connu pour être un important carrefour du trafic illicite de stupéfiants. L'un d'eux a également déposé de l'argent liquide sur son compte auprès d'une banque en Belgique. Les opérations atypiques des personnes concernées et leur profil de risque accru en matière de corruption et d'implication dans la criminalité organisée transfrontalière liée au milieu des stupéfiants ont conduit à soupçonner que l'argent en espèces déposé provenait de la corruption et de la criminalité organisée.

La CTIF a constaté que, dans plusieurs cas, les produits de la corruption et du détournement de fonds avaient été investis dans l'immobilier ou utilisés pour financer des rachats d'entreprises. Une fois encore, des achats d'autres biens de grande valeur, notamment des véhicules de luxe, ont été observés, ainsi que des transactions indiquant des activités de jeu dans des casinos ou des salles de jeux. Comme la CTIF l'a souligné à plusieurs reprises, les professions non financières jouent un rôle crucial dans la détection de ces opérations de blanchiment et leur déclaration à la CTIF.

Il ressort de quelques dossiers que les personnes concernées ont effectué des virements en faveur de prestataires de services de crypto-actifs dans l'UE, convertissant ainsi des avoirs obtenus illégalement en monnaie virtuelle. Cette fréquence limitée ne signifie pour autant pas que les cryptomonnaies sont à l'abri de la corruption. Cela semble plutôt démontrer que le rôle des actifs virtuels en tant qu'instrument de blanchiment des produits de crimes liés à la corruption prend progressivement de l'ampleur.

Dans le cadre de ses analyses sur la corruption et le détournement de fonds, la CTIF a recueilli des renseignements (complémentaires) auprès de divers partenaires, notamment des entités assujetties, des services de police et des autorités judiciaires. Dans un certain nombre de dossiers spécifiques, des informations ont également été demandées aux services de renseignement et de sécurité ou à l'Office européen de lutte antifraude de la Commission européenne.

La majorité des dossiers transmis par la CTIF présentaient une dimension transnationale manifeste, en raison de la nature et des activités des personnes impliquées et/ou des transactions financières. Dans de tels dossiers, la coopération internationale constitue un élément essentiel et indispensable de l'analyse réalisée par la CTIF. Dans de nombreuses analyses, les renseignements obtenus par l'intermédiaire d'autres CRF ont joué un rôle significatif.

La CTIF a également informé en 2025 des CRF étrangères de transactions suspectes impliquant des PPE dans leur pays. Cela s'est principalement fait en application de l'article 53, paragraphe 1, de la quatrième directive européenne LBC/FT et dans le cadre du traitement des déclarations reçues concernant les relations de correspondance bancaire.

Criminalité informatique

En 2025, plus de 90% des dossiers transmis par la CTIF en lien avec la criminalité informatique concernaient **l'achat d'images d'abus sexuels sur mineurs**. Outre l'achat de matériel numérique représentant des abus réels, certains dossiers portaient sur l'achat d'images réalistes de mineurs fictifs (par exemple des films d'animation à caractère sexuel mettant en scène des mineurs) et sur du matériel représentant des personnes d'apparence mineure (notamment des poupées sexuelles à l'apparence enfantine). Quelques dossiers concernaient la vente d'images à caractère sexuel produites par des mineurs (contenu auto-généré).

A l'instar de l'année passée, plusieurs dossiers ont été initiés sur base d'informations provenant principalement de partenaires étrangers. En raison de la nature transnationale des réseaux criminels, la CTIF a étroitement coopéré avec ses homologues étrangers. En retour, elle a partagé des informations avec plusieurs CRF étrangères.

Bien que différents modes de paiement soient observés, les transactions les plus fréquentes s'effectuent via des établissements de monnaie électronique ou de transfert de fonds de type *money remittance*. Les cryptomonnaies ont été utilisées dans une moindre mesure.

Les montants unitaires sont souvent faibles. Il s'agit généralement de montants ronds compris entre 15 et 100 EUR par transaction effectuée par des intervenants n'ayant aucun lien de parenté avec le bénéficiaire.

Les transactions s'accompagnent parfois de communications faisant référence à la taille des fichiers ou renvoyant à des comptes de réseaux sociaux ou services de messagerie. Cela semble indiquer que ces services et, par extension, d'autres applications de communication chiffrées de bout en bout ont créé d'importantes possibilités de mise en réseau pour les auteurs.

Les autres dossiers transmis par la CTIF en lien avec la criminalité informatique concernent, d'une part, des transactions financières liées à des activités illicites de fourniture de services liés à l'IPTV et, d'autre part, des opérations frauduleuses liées à une plateforme de trading décentralisée de crypto-actifs.

La criminalité environnementale

La criminalité environnementale couvre un **large spectre** d'activités illicites parmi lesquelles l'exploitation forestière illégale, le commerce illégal d'espèces sauvages, le trafic de déchets et l'exploitation minière illégale. Ils affectent à la fois les écosystèmes, les économies et la stabilité des sociétés humaines en se nourrissant des opportunités créées par leur réalité internationale.

Le groupe Egmont[17] et le rapport EU SOCTA 2025[18] soulignent que la criminalité environnementale est considérée comme l'un des crimes les plus rentables au monde. Elle constitue une source de revenus particulièrement attractive pour les réseaux criminels qui s'appuient sur des stratégies sophistiquées et transnationales pour perpétuer leurs activités illégales.

[17] (Egmont, 2025) IEWG Project - FIU Role in Fighting Environmental Crimes
[18] (Europol, 2025) : https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

Le Livre blanc sur la criminalité financière[19], auquel la CTIF a contribué, met en lumière l'utilisation de structures commerciales légales comme façade, l'exploitation des failles juridiques internationales, la corruption et le recours à des techniques complexes de blanchiment de capitaux. Dans le cadre de la lutte contre cette criminalité, les CRF peuvent jouer un rôle clé grâce à l'analyse des flux financiers illicites.

L'expérience actuelle de la CTIF est relativement limitée car elle repose sur un faible nombre de déclarations de soupçon liées à des infractions environnementales. Ce faible nombre met en lumière la **complexité des schémas financiers** impliquant que les transactions associées aux crimes environnementaux s'intègrent souvent dans des chaînes économiques légales, rendant leur identification plus difficile.

Malgré le nombre limité de déclarations de soupçon, la CTIF a transmis plusieurs dossiers aux autorités judiciaires. L'analyse des dossiers révèle que si certains crimes environnementaux sont de nature opportuniste et occasionnelle, d'autres impliquent des réseaux criminels organisés qui ont recours à des techniques de blanchiment sophistiquées.

Une partie des dossiers est caractérisée par une composante environnementale évidente et concerne des opérations de blanchiment que la CTIF a pu mettre en lien direct avec le **trafic d'espèces sauvages**, le trafic de bois ou le trafic de déchets. Dans une autre partie des dossiers, la composante environnementale apparaît davantage en arrière-plan et la CTIF identifie principalement des indices sérieux de blanchiment de capitaux liés à d'autres formes de criminalités sous-jacentes, telles que la corruption ou le trafic illicite de biens et de marchandises.

1.2. Évolution des techniques de blanchiment

1.2.1. L'utilisation abusive des structures sociétaires comme vecteur de blanchiment

Les autorités politiques et judiciaires font de la lutte contre les sociétés écrans l'une de leurs priorités actuelles. La proposition de loi visant à modifier le Code des sociétés et des associations afin d'accélérer les procédures et d'étendre les causes de dissolution judiciaire en est un exemple récent. Trouver l'équilibre entre la réalité économique, qui vise à encourager l'entrepreneuriat, et la nécessité de lutter contre l'utilisation abusive des structures sociétaires comme vecteur de blanchiment polycriminel constitue un véritable défi.

Depuis de nombreuses années, la CTIF œuvre activement au processus de détection préventive de ces sociétés frauduleuses sur la base de ses dossiers et grâce à une collaboration soutenue avec ses différents partenaires.

La CTIF poursuit ses efforts afin de détecter les sociétés écrans nouvellement constituées. Cette initiative s'appuie sur les recommandations formulées par le GAFI dans le rapport d'évaluation mutuelle de la Belgique[20].

Le recours à des sociétés ayant une activité réelle partiellement illicite

Une partie des dossiers implique l'utilisation de sociétés exerçant une activité économique réelle dont une partie est réalisée de manière illicite à des fins de fraude sociale et fiscale grave, de traite des êtres humains ou d'abus de biens sociaux.

[19] Livre blanc : systématiser les investigations financières pour combattre la criminalité environnementale en Europe, Sous la direction de Chantal Cutajar, Dalloz, 2025.
[20] https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Evaluation-mutuelle-Belgique-2025.pdf.coredownload.inline.pdf (p.121)

Si les secteurs d'activités correspondent à des secteurs réputés sensibles en matière de fraude sociale et fiscale, tels que la construction et le nettoyage industriel, la CTIF a constaté un recours croissant, en 2025, au secteur des travaux liés à l'installation de réseaux de télécommunications ainsi qu'à d'autres secteurs, tels que celui des boulangeries. Associée aux techniques de compensation et de blanchiment de capitaux basé sur le commerce (*Trade-based Money Laundering* ou *TBML),* la mixité des fonds provenant, d'une part, de transferts issus des activités licites de ces sociétés et, d'autre part, de fausses facturations, est réalisée dans le but de compliquer la traçabilité des fonds.

La CTIF a également constaté le recours croissant à des sociétés actives dans la prestation de certains services (informatique, marketing, sécurité, transport, conseil, etc.). Dans les dossiers concernés, les paiements relatifs au service fourni sont justifiés par des factures de service dont il est particulièrement difficile de déterminer si elles sont réelles ou fictives. Cette technique correspond au blanchiment basé sur les services (*Service-Based Money Laundering* ou *SBML*). À la différence du TBML, le SBML consiste à déplacer ou à justifier des fonds d'origine illicite par le biais de transactions commerciales liées non pas à des marchandises mais à la prestation de services.

Le recours à des sociétés écrans de compensation

Au cours des dernières années, la CTIF a observé la création ou la reprise de sociétés dans le but de blanchir des fonds d'origine illicite par la technique de la compensation. Il s'agit en particulier de dossiers de type « filières », liés à la **criminalité organisée, à la fraude fiscale grave et à la fraude sociale.**

Ces dossiers se caractérisent par le rôle central joué par des sociétés écrans, constituées en série, actives dans des secteurs sensibles en matière de fraude sociale et fiscale (construction, hôtellerie-restauration, nettoyage, transport, viande, etc.) et qui n'ont souvent aucune activité économique.

L'objectif poursuivi en utilisant ces sociétés est purement de faciliter le blanchiment par un échange d'argent liquide entre des criminels qui en génèrent beaucoup (notamment en lien avec le trafic de stupéfiants) et des criminels à la recherche d'argent liquide afin, notamment, de rémunérer une main-d'œuvre non déclarée.

Les schémas les plus complexes reposent sur une constellation de sociétés et de comptes bancaires mis en place par des blanchisseurs professionnels ; des facilitateurs (professionnels de la finance, du droit et de la comptabilité) instrumentalisés par les criminels dans le cadre de leurs missions ; un grand nombre d'hommes de paille et de mules, en Belgique comme à l'étranger.

Outre l'utilisation de sociétés écrans dans les dossiers de compensation en lien avec la criminalité organisée, la fraude sociale et fiscale grave, la CTIF a pu établir, cette année, des liens avec la **traite des êtres humains et l'exploitation de la prostitution**. Ce constat confirme ainsi ce qu'avait publié Myria dans son rapport 2024[21].

Divers éléments confirment la dimension de traite des êtres humains et d'exploitation de la prostitution dans ces dossiers. Il s'agit, d'une part, de l'implication d'agences de voyages qui reçoivent d'importantes sommes d'argent, via les sociétés créées par ce réseau professionnel de blanchiment, en vue de payer les vols qui transportent les victimes d'Amérique latine (attirées au préalable par les réseaux sociaux) vers la Belgique et d'autres pays européens. Il s'agit, d'autre part, de preuves multiples de paiements de loyers apparaissant sur les relevés des comptes des sociétés écrans. Dans ces dossiers, on observe également que s'allient tant les nouvelles technologies que les techniques plus traditionnelles pour attirer les victimes et blanchir les capitaux.

[21] Myria, Rapport 2024, Travail du sexe latino-américain : un carrousel à risques https://www.myria.be/files/2024_MYRIA_Rapport_annuel_Traite_et_trafic_des_%C3%AAtres_humains.pdf

1.2.2. Paiements pour le compte de tiers ou third party payments (TPP)

Lors de l'analyse des réseaux internationaux de blanchiment de capitaux, le recours aux paiements effectués par des tiers apparaît de plus en plus important. En substance, les TPP se définissent comme des paiements réalisés par un tiers (*third party*) sur ordre ou pour le compte d'un payeur (*payer*) au profit d'un bénéficiaire (*payee*).

Dans le cadre des transactions financières licites, plusieurs prestataires de TPP ont émergé au cours des dix dernières années. Il s'agit d'établissements de paiement qui, moyennant rémunération, prennent en charge l'exécution et la gestion des obligations de paiement pour le compte de leurs clients. Les frais appliqués aux transferts ainsi que les taux de change proposés sont souvent plus avantageux que ceux des systèmes de paiement traditionnels. Les TPP sont également utilisés depuis longtemps pour effectuer des paiements à destination et en provenance de régions où l'accès au système bancaire est limité.

Les criminels ont rapidement saisi les opportunités offertes par l'essor et la normalisation des canaux de paiements alternatifs. Dans le cadre du blanchiment de capitaux, les TPP sont ainsi utilisés pour masquer les liens financiers et rendre le suivi des flux financiers plus difficile, y compris dans les régions où le système bancaire est pleinement accessible.

Les réseaux professionnels de blanchiment recourent aux TPP en les combinant avec la technique de la compensation, notamment dans des schémas de TBML ou de SBML.

1.2.3. Banque souterraine et systèmes informels de transfert de valeur (IVTS)

Au fil du temps, le processus de blanchiment s'est progressivement dissocié, voire autonomisé, par rapport aux activités criminelles génératrices de revenus d'origine illicite, favorisant notamment le développement de systèmes financiers alternatifs en dehors des institutions financières légalement réglementées.

L'ensemble des activités financières opérant en dehors du cadre réglementaire officiel utilise divers mécanismes afin de contourner le secteur réglementé pour transférer des fonds au niveau international, sans nécessairement les déplacer physiquement. Ces activités sont désignées par le terme générique d'*underground banking* [22] .

Si ces systèmes « souterrains » fonctionnent sur le même principe que les systèmes informels de transfert de valeur - *Informal Value Transfer Systems* ou *IVTS* - de type *hawala*, ils se sont toutefois professionnalisés afin d'offrir des services de blanchiment à grande échelle.

Le réseau *hawala* est un système informel de transfert de fonds qui repose sur la confiance entre les intermédiaires appelés hawaladars. Ce système est souvent utilisé pour envoyer de l'argent rapidement et discrètement à travers les frontières, sans laisser de traces électroniques ou documentaires. Les caractéristiques du réseau *hawala* le rendent attractif pour les travailleurs immigrés, les personnes n'ayant pas accès au système bancaire traditionnel, mais également pour les groupes criminels ou terroristes qui bénéficient de son anonymat.

La compensation entre les deux hawaladars s'effectue ensuite de diverses manières : les plus fréquentes incluent les compensations en espèces et les compensations commerciales (des surfacturations peuvent notamment compenser les valeurs transférées). Notons que les banquiers clandestins utilisent de plus en plus la cryptomonnaie comme moyen de transfert de valeur intermédiaire, apportant une dimension de modernité au système de compensation de valeurs connu.

Contrairement aux techniques sophistiquées de blanchiment mêlant sociétés écrans, prête-noms, comptes offshore et ingénierie financière, l'IVTS est un instrument qui répond surtout aux besoins des

[22] Lien vers Vademecum

criminels cherchant à blanchir d'importantes quantités d'argent liquide. En effet, en raison de leur fonctionnement largement informel et de l'absence de traçabilité des opérations, ces **systèmes financiers parallèles** offrent un cadre particulièrement propice au blanchiment de capitaux et permettent d'absorber et de redistribuer d'importantes quantités d'argent liquide sans recourir aux canaux bancaires traditionnels. Cette capacité à traiter des volumes élevés de liquidités, tout en dissimulant leur provenance, confère à ces systèmes un rôle clé dans les stratégies contemporaines de blanchiment de capitaux.

Les risques de blanchiment en Belgique trouvent leur origine, en partie, dans des réseaux financiers alternatifs, qui se développent en dehors du champ réglementé de la LBC et des acteurs soumis à ce dispositif[23] .

Ces menaces sont donc difficilement mesurables et quantifiables, même si leur existence et leur ampleur sont avérées, notamment grâce aux actions policières qui révèlent ces activités.

En 2025, l'expérience de la CTIF confirme l'implication de réseaux clandestins *hawala* dans plusieurs dossiers transmis. Grâce aux informations policières et judiciaires, aux renseignements obtenus auprès des services de renseignement ou d'autres CRF, la CTIF a pu établir des liens entre, d'une part, des opérations financières suspectes détectées sur des comptes bancaires en Belgique et, d'autre part, des services financiers fournis par des réseaux d'hawaladars.

Plusieurs dossiers transmis en 2025 visent ainsi des personnes physiques multi-bancarisées installées en Belgique dont les comptes bancaires ont enregistré de nombreux flux financiers ainsi que des versements en espèces alors qu'aucune activité professionnelle déclarée ne pouvait justifier ces opérations. Leurs comptes bancaires ont été principalement crédités par des virements et débités par des transferts vers l'étranger. Des informations reçues notamment des services de renseignement ont permis de relier ces personnes à un réseau d'hawaladars actif en Belgique.

Ces dossiers ont notamment été transmis pour blanchiment de capitaux provenant de la fourniture de services bancaires, de transferts de fonds ou du commerce de devises sans disposer de l'agrément requis ou des conditions d'accès pour l'exercice de ces activités.

1.2.4. Transaction Laundering

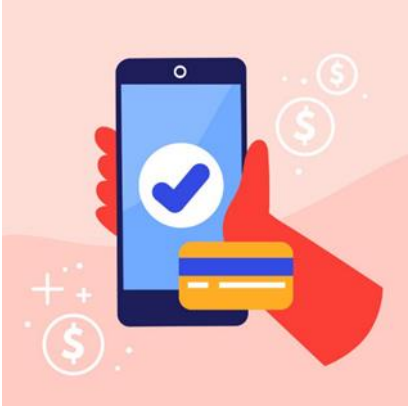
Au cours des dix dernières années, la part du commerce en ligne en Belgique a fortement progressé, avec un pic particulièrement marqué après la période de la Covid. En 2025, le marché total du commerce électronique dans notre pays aurait atteint près de 25 milliards d'euros, et plus de 75 % des Belges auraient effectué des achats en ligne[24]. Parallèlement au développement du commerce en ligne, les possibilités de paiement numérique et de paiement en ligne ont également connu une croissance spectaculaire.

Au vu de ces chiffres, il n'est pas surprenant que la CTIF relève, dans ses dossiers de 2025, de plus en plus d'indices, d'une forme ou d'une autre, de blanchiment de capitaux pouvant être liés au commerce en ligne ou e-commerce, et plus particulièrement aux solutions de paiement qui y sont associées.

Les techniques de blanchiment utilisées dans le commerce physique de biens (TBML) et de services (SBML) ont en effet des équivalents dans le commerce en ligne. Elles reposent sur le même principe, à savoir la dissimulation de flux financiers illicites par le biais du commerce de biens ou de services. Les différentes formes de blanchiment de capitaux via le commerce et les paiements en ligne sont généralement repris sous le terme de *transaction laundering.*

[23] https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Evaluation-mutuelle-Belgique-2025.pdf.coredownload.inline.pdf
[24] https://economie.fgov.be/fr/themes/line/economie-numerique-en-chiffres

Le *transaction laundering* désigne le fait d'utiliser ou de détourner les systèmes de paiement de boutiques en ligne ou d'entreprises d'apparence légitimes pour faire transiter des transactions financières illégales. Les paiements liés à des activités illégales (ventes de produits contrefaits, armes, jeux d'argent non autorisés, …) sont ainsi traités via le compte du commerçant d'apparence légale sans que l'acquéreur[25] (*acquirer* ou *merchant acquirer)* en ait connaissance. Cela enfreint le contrat conclu entre le commerçant et l'acquéreur, vu que des sites illégaux utilisent les facilités de paiement prévues pour un commerçant légitime afin de dissimuler leurs transactions.



Comme le rôle de l'acquéreur se situe à la croisée des chemins entre le technologique et le financier, et que certains sous-processus peuvent être externalisés (tâches sous-traitées), il n'est pas toujours évident de déterminer où se situent les responsabilités en matière de conformité (contrôles lors de l'intégration de nouveaux clients/boutiques en ligne, *Know Your Customer*, *Know Your Transaction*, etc.).

Les criminels peuvent exploiter la complexité du commerce en ligne pour mener des activités illégales et blanchir les revenus qui en découlent. Ainsi, les paiements réalisés au profit d'un marchand en ligne, vendant de la drogue ou d'autres produits illégaux, peuvent sembler provenir d'une boutique en ligne légale. Les paiements liés à des activités de jeux d'argent illégaux peuvent également transiter par des sites web discrets. Les paiements issus de fraudes à l'abonnement – escroquerie consistant à faire croire aux clients qu'ils effectuent un paiement unique alors que leur carte de crédit est débitée périodiquement – peuvent être présentés comme des paiements légitimes. Le nombre élevé de *chargebacks* ou de demandes de remboursement par le client constitue un indice fort d'escroquerie et dès lors de *transaction laundering.*

Compte tenu de la croissance du commerce en ligne et du développement des technologies financières destinées au traitement de ces transactions, le phénomène du Transaction Laundering semble appelé à prendre de l'ampleur à l'avenir et restera un sujet de préoccupations majeures pour la CTIF.

1.2.5. Actifs virtuels

A l'instar des dossiers impliquant le blanchiment de monnaie fiduciaire (Fiat), la CTIF constate, dans les dossiers liés aux cryptomonnaies, que les intervenants anticipent le risque potentiel d'un contrôle de leurs actifs et tentent de complexifier leurs transactions. Ils ouvrent ainsi des comptes auprès de **prestataires de services offshore liés aux crypto-actifs** (par exemple, des plateformes de jeux de hasard offshore ou plateformes d'échange de cryptomonnaies offshore) et utilisent différentes techniques pour rendre leurs transactions anonymes.

On remarque notamment le recours fréquent à des prestataires de services de crypto-actifs problématiques. Ces prestataires mélangent souvent les cryptomonnaies de différents clients dans ce qu'on appelle des « portefeuilles de grand livre », ce qui rend alors impossible l'identification de l'origine individuelle des cryptomonnaies à partir d'une analyse de la blockchain publique. Les données internes de ces entités sont nécessaires pour pouvoir retracer l'origine ou la destination des cryptomonnaies qui ont transité par ces plateformes. C'est notamment pour cette raison que, dans plusieurs juridictions, les prestataires de services liés aux crypto-actifs ont l'obligation d'identifier leurs clients, de surveiller les transactions et de répondre aux demandes des autorités qui enquêtent sur l'origine des dépôts ou la destination des retraits. Les criminels en sont conscients et exploitent les plateformes établies dans des juridictions où ces normes ne sont pas respectées.

[25] L'acquéreur sert d'intermédiaire entre le commerçant, les réseaux de paiement (comme Visa, Mastercard, etc.) et la banque du client en ligne. Cet acteur joue un rôle essentiel dans l'écosystème des paiements en ligne. C'est lui qui entre autres garantit le transfert des fonds du compte bancaire du client vers celui du commerçant.

Dans les dossiers d'escroquerie et ceux concernant les « mules financières », la CTIF constate régulièrement la conversion par les criminels de l'argent des victimes en cryptomonnaies, puis leur transfert vers des plateformes offshore d'échange où sa destination finale est dissimulée dans la mesure où les cryptomonnaies sont mélangées à celles des autres clients de la plateforme et que celle-ci ne coopère pas avec les autorités. Le même mode opératoire est également constaté pour les cryptomonnaies provenant de la vente d'images d'abus sexuels sur mineurs, ainsi que dans les dossiers relatifs au financement du terrorisme.

Le recours récurrent à des plateformes de jeux de hasard offshore utilisant des cryptomonnaies est également observé. Ces plateformes acceptent les dépôts et retraits en cryptomonnaies et proposent des jeux d'argent équivalents à ceux des opérateurs réglementés. Ne disposant pas d'une licence délivrée par la Commission des jeux de hasard, elles ne sont pas autorisées à exercer en Belgique. Cependant, certains utilisateurs belges contournent cette interdiction, notamment via des connexions VPN.

Dans la pratique, l'ouverture de tels comptes est relativement facile. En effet, les plateformes de jeux de hasard non réglementées exigent peu voir aucune information d'identité de leurs clients et ne vérifient pas si ceux-ci sont soumis à une interdiction nationale.

Le recours aux plateformes d'échange de cryptomonnaies et de jeux de hasard basées sur la cryptomonnaie est fréquent dans les dossiers liés aux actifs virtuels.

Outre le recours abusif à des prestataires de services offshore, la CTIF observe, comme les années précédentes, l'utilisation continue de techniques structurellement liées à la criminalité et au blanchiment de capitaux. **Les mixeurs de cryptomonnaies** servent notamment à dissimuler les cryptomonnaies qui y transitent. En effet, les utilisateurs de ces mixers mélangent leurs cryptomonnaies avec celles de tiers. Lorsque les cryptomonnaies quittent le mixer, il est plus difficile de déterminer quels actifs appartiennent à quel expéditeur et à quel destinataire.

Les criminels exploitent également des programmes déployés sur la *blockchain* qui, bien que conçus pour des usages légitimes, compliquent la traçabilité des cryptomonnaies. Dans la majorité des dossiers liés aux cryptomonnaies, on constate l'implication des plateformes DeFi, c'est-à-dire des **plateformes de finance décentralisée**. Ces plateformes permettent des opérations financières via des applications en ligne sans autorité centrale : elles sont gérées collectivement par une communauté d'utilisateurs qui, ensemble, font fonctionner la plateforme. Outre l'échange de cryptomonnaies, la CTIF constate que les intervenants belges participent également, via ces plateformes, à des enchères concernant des ***Non Fungible Tokens***[26] (NFT), et contractent des prêts ou placent des paris. La gestion décentralisée par différents utilisateurs de cryptomonnaies est rendue possible par ce que l'on appelle des contrats intelligents. Il s'agit de programmes inscrits sur la blockchain qui exécutent automatiquement et de manière autonome des transactions selon des règles prédéfinies.

Dans de nombreux dossiers, l'analyse du **statut fiscal** des interactions avec ces plateformes s'avère pertinente. En effet, certains intervenants belges transfèrent leurs actifs crypto hors de la gestion des plateformes d'échange crypto réglementées vers leurs propres **portefeuilles privés**, pour ensuite négocier ces actifs via des plateformes de trading décentralisées.

Il arrive régulièrement que des personnes se livrent à des activités spéculatives ou professionnelles liées aux cryptomonnaies, lesquelles sont soumises à un régime fiscal. La non-déclaration de ces revenus a conduit, à plusieurs reprises, à des transmissions aux parquets en raison de l'existence d'indices sérieux de blanchiment provenant de la fraude fiscale grave.

[26] NFT : jeton non fongible en français – est un certificat d'authenticité numérique enregistré sur une blockchain.

Des escrocs belges exploitent également les plateformes décentralisées pour faciliter leurs escroqueries et leurs opérations de blanchiment. Ainsi, la CTIF a identifié un cas où un intervenant belge a créé des tokens qu'il a mis en vente sur une plateforme de trading décentralisée. Peu après le lancement, l'intervenant a artificiellement gonflé le prix de ces tokens en en achetant lui-même via un portefeuille distinct. Au terme du schéma de fraude, il a rendu la vente de ces tokens impossible et s'est enfui avec les fonds des victimes, qui se sont retrouvées avec des tokens sans valeur.

Les dossiers relatifs aux cryptomonnaies traités par la CTIF montrent toutefois que les méthodes susmentionnées et la technicité du sujet ne garantissent pas aux criminels le succès de leurs opérations de blanchiment. Dans plusieurs dossiers, l'identité d'intervenants belges a pu être établie en lien avec les cryptomonnaies grâce au traçage des fonds à travers des mixeurs, des plateformes de cryptomonnaies, des plateformes de jeux d'argent et des plateformes décentralisées. Dans d'autres dossiers, le rôle prépondérant des organisateurs dans des schémas criminels à grande échelle a été mis en lumière et les parquets ont été informés de soldes en cryptomonnaies importants.

Les informations que la CTIF reçoit et collecte auprès de prestataires étrangers de services liés aux crypto-actifs, via l'échange de données avec les autres CRF, sont donc essentielles pour mettre au jour le blanchiment et les infractions commises via des transactions en cryptomonnaies. La CTIF peut valoriser pleinement ce rôle grâce à une spécialisation continue et à une coopération constante avec les CRF. Cette année encore, les collaborateurs de la CTIF se sont régulièrement réunis avec leurs homologues étrangers afin d'échanger des connaissances opérationnelles sur les dossiers liés aux cryptomonnaies et renforcer l'approche stratégique en matière de blanchiment et de financement du terrorisme via les transactions en cryptomonnaies.

1.2.6. Immobilier

L'analyse nationale des risques identifie les investissements immobiliers en Belgique ou à l'étranger parmi les principaux risques en matière de blanchiment en Belgique.

La CTIF observe depuis de nombreuses années que l'immobilier constitue une méthode privilégiée pour intégrer des fonds issus du trafic de stupéfiants, de la criminalité organisée, de la fraude fiscale grave et de la fraude sociale ainsi que de la corruption, tant en Belgique qu'à l'étranger.

Les dossiers révèlent l'utilisation et la combinaison de plusieurs techniques par des réseaux de blanchisseurs professionnels. Ces méthodes incluent notamment le transport d'argent liquide, l'injection de capitaux dans des sociétés actives dans des secteurs considérés à risque, le blanchiment par compensation, le blanchiment basé sur le commerce et le paiement pour le compte de tiers.

L'investissement immobilier, tant en Belgique qu'à l'étranger, représente souvent la dernière étape du service fourni par le réseau de blanchisseurs professionnels.

Cette année encore, les dossiers mettent en évidence une distinction entre les investissements immobiliers nationaux et internationaux. Dans le cas des investissements immobiliers nationaux, les montants sont généralement moins élevés et les techniques utilisées moins complexes. Il s'agit d'investissements directs de fonds d'origine illicite, de prêts auprès d'amis ou de la famille. Les biens immobiliers peuvent également être acquis dans le but d'être loués ou d'accueillir des activités commerciales.

Les investissements à l'étranger, quant à eux, s'inscrivent fréquemment dans un schéma de blanchiment international orchestré par un réseau professionnel de blanchiment. Les investissements immobiliers représentent alors le dernier maillon du processus de blanchiment. Des prestataires de services locaux tels que des agents immobiliers, des sociétés de conseil ou des cabinets d'avocats sont souvent utilisés, jouant le rôle de facilitateurs pour acquérir le bien. Cependant, des cas ont également été observés dans lesquels les dirigeants d'organisations criminelles basées en Belgique ont acquis des biens immobiliers à l'étranger en leur nom propre ou par le biais de leurs sociétés.

En 2025, la CTIF a particulièrement renforcé ses contacts avec ses homologues étrangers afin de partager des expériences concernant les typologies rencontrées en matière d'investissements immobiliers.

2. Tendances en matière de financement du terrorisme

Contexte

Les facteurs contextuels déterminent dans une large mesure les risques spécifiques de financement du terrorisme auxquels une juridiction est exposée. Du point de vue de la CTIF, les tendances géopolitiques, associées à la numérisation accrue et aux évolutions technologiques au sein de l'infrastructure financière, constituent un sujet de préoccupation spécifique. Non seulement les médias numériques réduisent la distance avec la zone de conflit, mais le monde en ligne et les réseaux sociaux peuvent également favoriser les processus de radicalisation, voire la planification d'attentats.

Ces évolutions vont de pair avec la transformation de l'écosystème financier. Dans un environnement numérique en constante expansion, des alternatives aux institutions financières et aux systèmes de paiement traditionnels voient le jour. Les applications *fintech* permettent à des plateformes qui, à l'origine, ne poursuivent aucune finalité financière, de s'insérer dans le paysage des paiements. La monétisation de cette connectivité numérique fait ainsi émerger un champ de tension entre propagande, radicalisation et financement, s'inscrivant dans une dynamique d'une menace bien réelle.

Collecte de fonds et nouveaux moyens de paiement

La collecte de fonds demeure un élément central des enquêtes relatives au financement du terrorisme. Traditionnellement, ces collectes sont coordonnées par des organisations à but non lucratif, des institutions religieuses ou des fondations. Toutefois, le lien entre la collecte de fonds et les réseaux sociaux, combiné aux nouvelles technologies de paiement, a considérablement élargi la portée et l'impact des campagnes de collecte, les rendant accessibles à tous. Le risque réside principalement dans la collecte de fonds en apparence légitime dans une zone à faible risque, avant leur transfert vers des juridictions à haut risque via une chaîne de services financiers (non réglementés) tels que le transport transnational d'espèces, le *hawala* ou les plateformes d'échange et de mixage de cryptomonnaies.

La CTIF reste donc vigilante quant à la détection d'indices, lors des transferts de fonds vers des juridictions à risque, susceptibles d'indiquer le recours à des passeurs, à des sociétés facilitant les transferts d'argent, à des pratiques de *hawala* ou à l'utilisation de bureaux de change. Ces pratiques demeurent une source de financement très réelle.

En raison des importantes évolutions dans le domaine numérique, le risque d'utilisation abusive des nouveaux moyens de paiement par des organisations terroristes et des particuliers s'est accru. Dans ses dossiers, la CTIF observe, outre le recours aux institutions financières traditionnelles, une utilisation croissante des PSP et des établissements de monnaie électronique. Ces méthodes de paiement sont désormais largement répandues et acceptées, mais elles requièrent une vigilance

accrue car leur facilité d'utilisation et leur accessibilité les rendent vulnérables à des abus notamment en matière de financement du terrorisme.

La collecte de fonds reste un élément central des enquêtes en matière de financement du terrorisme.

La large gamme d'établissements ou d'outils, tels que les IBAN virtuels (VIBAN), qui facilitent les transactions transfrontalières grâce à de faibles frais de change, constitue également une tendance manifeste. Il n'est pas rare que les transactions soient « fractionnées » et réparties entre différents établissements de paiement dans plusieurs juridictions. Cette pratique semble répondre à une recherche accrue d'autonomie financière, et par extension d'invisibilité financière, en fractionnant les transactions entre différentes juridictions afin de maximiser les avantages juridiques, financiers et personnels.

Actifs virtuels

Conformément aux évolutions technologiques observées, la CTIF a également constaté une augmentation de l'utilisation des actifs virtuels dans les dossiers externalisés. À mesure que les actifs dématérialisés gagnent en popularité, leur utilisation par les groupes terroristes et les terroristes individuels tend également à s'intensifier. Cette évolution se traduit, d'une part, par le nombre croissant de transactions impliquant des crypto-actifs et, d'autre part, par les différentes applications rendues possibles par celles-ci. La rapidité des transactions, combinée à l'usage fréquent de multiples plateformes réparties dans différentes juridictions compliquent la traçabilité de l'origine, de la destination et des bénéficiaires finaux des fonds. La nature décentralisée et immatérielle des actifs virtuels accentue les risques d'utilisation à des fins de financement du terrorisme. Leur caractère hautement technologique constitue également un défi majeur en matière de détection. Afin de faire face à ces défis, la CTIF s'emploie donc à renforcer davantage l'échange d'informations tant avec ses partenaires nationaux qu'au sein des initiatives de coopération internationale.

Systèmes informels de transfert de valeur (IVTS)

La CTIF constate, en concertation avec ses partenaires en charge de la sécurité nationale, une complexification croissante des structures de financement. Le parquet fédéral a notamment mis en évidence l'utilisation conjointe de systèmes informels de transfert de valeur – des systèmes financiers alternatifs tels que le *hawala* numérique – et de cryptomonnaies[27]. Les transformations numériques de méthodes de paiement autrefois traditionnelles, telles que les services de transfert d'argent (de type *money remittance*), qui au-delà des transferts traditionnels au guichet et leurs virements, proposent désormais des options de transfert mobile, constituent également un facteur de risque. L'émergence de nouvelles méthodes de paiement, d'infrastructures financières technologiques avancées et d'actifs virtuels semble donc perturber les structures classiques des typologies existantes en matière de financement du terrorisme. Si la fonction principale du *hawala* demeure inchangée, sa forme numérique pourrait en accroître l'ampleur, la rapidité et la complexité.

Certaines structures de transfert de fonds adoptent un modèle hybride, combinant les outils numériques avec ceux des institutions financières traditionnelles. La CTIF a pu identifier un certain nombre de dossiers liés à la prestation de services bancaires, de transfert de fonds ou de change sans disposer de l'agrément requis pour ces activités, ainsi qu'à des opérations de financement du terrorisme.

Financement du terrorisme lié au commerce (TBTF)

Enfin, en 2025, la CTIF a traité plusieurs dossiers dans lesquels il était question de *crime-terror nexus*. Le mode opératoire identifié reposait sur un financement du terrorisme basé sur le commerce (*Trade-*

[27] Parquet fédéral, rapport annuel 2024.

Based Terrorism Financing ou *TBTF*), une technique consistant à convertir et à transférer des fonds par le biais de transactions commerciales à des fins terroristes. Les transactions commerciales concernées peuvent provenir de sources aussi bien illégitimes que légitimes. Les sociétés belges impliquées agissent comme intermédiaires au sein d'un réseau international particulièrement étendu. Grâce à l'expertise de la CTIF en matière de détection des réseaux de blanchiment, il a été possible de mettre en évidence un schéma selon lequel des opérations entrantes sur les comptes de sociétés correspondaient à des revenus provenant de secteurs à forte intensité de main-d'œuvre, tels que la construction ou le nettoyage. Ces flux financiers étaient justifiés par de fausses factures, les fonds étant ensuite transférés vers d'autres sociétés tant en Belgique qu'à l'étranger. Dans les dossiers traités par la CTIF, il est apparu qu'au moins une de ces sociétés faisait l'objet d'une enquête judiciaire internationale relative au financement du terrorisme.

3. Contexte international

3.1 Contournement des sanctions

Les États et/ou les ressortissants de ces Etats faisant l'objet de sanctions financières tentent de contourner les sanctions financières mises en place à leur encontre en utilisant notamment de façon abusive le système de paiement pour compte de tiers, profitant du fait que les sociétés actives dans le commerce international recourent habituellement à la réception de paiements provenant d'autres parties que les acheteurs réels.

Ainsi, en échange d'une faible commission, des réseaux de contournement de sanctions offrent des services de paiement dans des domaines où le système financier régulier fonctionne parfaitement, en parvenant à mélanger des transactions en violation des sanctions financières avec des paiements s'inscrivant dans le cadre du commerce légitime.

Dans le cadre de ses compétences, la CTIF est plus fréquemment confrontée à la problématique du contournement des sanctions. Les dossiers concernés font l'objet d'une analyse approfondie et les informations pertinentes sont partagées avec les services belges compétents mais aussi avec ses homologues étrangers concernés.

Lorsque l'analyse de la CTIF met en lumière ce type d'agissements, elle a ainsi la possibilité de partager ces informations avec l'Administration générale de la Trésorerie du SPF Finances. Ces communications s'inscrivent dans le cadre de la mise en œuvre des sanctions financières, des embargos et des mesures restrictives qui sont pris par les Nations Unies, l'UE ou la Belgique à l'encontre de pays, de personnes ou d'entités dans le but de mettre fin aux violations de la paix et de la sécurité internationales telles que le terrorisme, les violations des droits de l'homme, la déstabilisation d'États souverains et la prolifération d'armes de destruction massive.

Dans ce cadre, la CTIF a communiqué des informations à l'Administration générale de la Trésorerie du SPF Finances à 4 reprises en 2023, 3 reprises en 2024 et 6 reprises en 2025.

Ces communications font généralement, mais pas exclusivement, suite à la transmission de dossiers aux autorités judiciaires. Dans ces dossiers, la CTIF met en avant des indices sérieux de blanchiment de capitaux en lien notamment avec le trafic illicite de biens et de marchandises, la fraude fiscale grave et/ou la fourniture de services bancaires, ou de transferts de fonds, sans disposer de l'agrément requis ou des conditions d'accès pour l'exercice de ces activités.

3.2. Évolution dans le domaine de la coopération européenne, FIU Next Gen, expert national détaché au titre de la LBA

Alors que 2024 pour l'AMLA était encore consacré à des travaux préparatoires concernant les locaux à Francfort et le recrutement de personnel, nous avons observé en 2025 que l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme a pris des mesures plus concrètes en matière de coordination et de soutien des CRF de l'UE.

Entre mars et décembre 2025, six réunions du Conseil général dans sa composition CRF (General Board in FIU composition) ont été organisées, soit en présentiel, soit par visioconférence. En sa qualité de chef de la CRF belge, le président de la CTIF a participé avec droit de vote à toutes ces réunions. Lors de ces séances, des questions relatives au fonctionnement pratique de l'AMLA ont été examinées et des décisions ont été prises, mais des étapes concrètes ont également été franchies pour mettre en œuvre les exigences du paquet AML.

Sur le plan organisationnel, nous citons le vote sur la nomination des membres du Conseil exécutif, à l'égard duquel il est très pertinent pour les CRF de noter qu'un membre du Conseil a démissionné et a été remplacé le 01/04/2026 par Hennie Verbeek-Kusters, l'ancienne cheffe de la CRF néerlandaise et également ancienne présidente du Groupe Egmont. Cette nomination a immédiatement renforcé les connaissances liées au monde des CRF au sein de l'AMLA. Le Conseil général a également approuvé les candidats pour les postes de délégués des CRF nationales. À titre de rappel : chaque CRF est tenue de détacher un collaborateur à Francfort, dont la rémunération reste à charge de la CRF nationale mais est affecté aux missions de l'AMLA. Pour la CTIF, ce rôle est occupé depuis le 01/01/2026 par un analyste. En ce qui concerne les discussions sur la composition et le rôle du Comité permanent (qui soutient le Conseil général dans sa composition CRF) ainsi que les droits et obligations des délégués des CRF, le président a fait entendre son avis à plusieurs reprises.

En matière de progrès et d'amélioration de la collaboration entre les CRF, plusieurs groupes de travail ont été mis en place et la CTIF a assuré, grâce à la participation de ses collaborateurs, de pouvoir peser techniquement et pratiquement sur ces sujets importants. Nous citons notamment : la méthodologie des analyses communes, l'assistance mutuelle, la médiation et l'examen par les pairs. En sa qualité de président du Groupe consultatif de FIU.net, le secrétaire général de la CTIF a joué un rôle moteur en facilitant l'accès de l'AMLA à FIU.net et en développant de nouvelles fonctionnalités qui permettront à l'AMLA d'exercer ses missions à l'avenir. Le transfert de l'hébergement et de la gestion de FIU.net à l'AMLA a également été engagé en 2025 et suivi de près par le secrétaire général de la CTIF.

En conclusion de la première année d'existence de l'AMLA, nous pouvons affirmer que l'Autorité a déjà réalisé de nombreux progrès en peu de temps, que l'intégration de tous les délégués des CRF est essentielle pour diffuser et renforcer la connaissance du monde des CRF au sein de l'AMLA, et que le rôle des CRF est de continuer à veiller au respect de leur autonomie et de leur indépendance en recherchant des solutions flexibles et coordonnées.

4. Contexte national

4.1. Évaluation mutuelle du GAFI

La fin d'année 2025 marque également la publication du rapport[28] d'évaluation mutuelle de la Belgique par le GAFI.

[28] https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Evaluation-mutuelle-Belgique-2025.pdf.coredownload.inline.pdf

Cette évaluation analyse en profondeur la mise en œuvre et l'efficacité des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive en Belgique. Une description du système belge de LBC/FT, ainsi que des recommandations ciblées pour le renforcer davantage, figurent dans ce rapport.

Les évaluations mutuelles comportent deux composantes principales : l'efficacité et la conformité technique.

- La partie la plus importante de l'évaluation est la notation de l'efficacité d'un pays et fait l'objet d'une visite sur place d'une équipe d'experts. Au cours de cette visite, l'équipe d'évaluation exige des preuves démontrant que les mesures du pays évalué fonctionnent et produisent les résultats attendus. Ce qui est attendu d'un pays varie en fonction des risques de blanchiment de capitaux, de financement du terrorisme et autres auxquels il est exposé.

- L'évaluation de la conformité technique constitue également une partie importante de l'évaluation mutuelle. Le pays évalué doit fournir des informations sur les lois, les règlements et tout autre instrument juridique mis en place pour lutter contre le blanchiment d'argent ainsi que le financement du terrorisme et de la prolifération des armes de destruction massive.

Etant donné le rôle central de la CTIF dans le système LBC/FT, les évaluateurs se sont également penchés sur plusieurs aspects fondamentaux liés aux renseignements financiers :

- Accès en temps opportun à des informations pertinentes, exactes et à jour
- Production et diffusion des renseignements financiers
- Coopération et échange d'informations et de renseignements financiers
- Utilisation des informations des renseignements financiers

La Belgique est notée comme ayant un niveau d'efficacité significatif dans ce domaine. L'équipe d'évaluation a fondé ses conclusions sur les cas présentés par les autorités, l'analyse des données statistiques disponibles, ainsi que sur les nombreux entretiens menés avec les autorités belges et les représentants du secteur privé.

4.2. Ateliers LBC/FT

La CTIF a développé en 2025 un nouvel outil de communication que sont les Ateliers LBC/FT afin d'améliorer le retour d'information vers les entités assujetties et répondre encore mieux aux attentes des déclarants**,** tout en complétant l'approche proposée depuis de nombreuses années.

Organisés par groupes sectoriels d'entités assujetties, l'objectif de l'Atelier LBC/FT est de partager des informations utiles aux déclarants qui pourraient faciliter la mise en œuvre des mesures préventives LBC/FT en abordant des typologies, études de cas, indicateurs ou toutes autres informations ciblées relatives au secteur.

L'Atelier permet de favoriser les échanges entre la CTIF, l'autorité de contrôle et les déclarants et de porter l'attention sur des sujets spécifiques en vue de sensibiliser davantage les déclarants sur des aspects LBC et ainsi parvenir à graduellement améliorer l'efficacité globale du processus préventif.

- Lors de la première édition des Ateliers LBC/FT, qui a eu lieu le 12 mai 2025, l'attention s'est portée sur le thème de la corruption en abordant l'aspect LBC préventif mais aussi répressif, couvrant ainsi le cycle de vie de la déclaration, allant du moindre soupçon, vers l'analyse et les potentiels indices sérieux de BC, et terminant en une potentielle enquête au Parquet. Proposé aux professions financières (les établissements de crédit et de paiement principalement), nous avons eu le plaisir d'accueillir, lors de cette 1ère édition de l'Atelier, la Cellule de renseignement financier française,

Tracfin, le Parquet fédéral ainsi que la Police fédérale qui ont pu partager leur expérience en matière de détection de la corruption à l'ensemble des nombreux participants présents.

Le succès de cette première édition s'est particulièrement mesuré à la richesse des échanges et à l'intérêt marqué de l'audience, qui s'est traduit par de nombreuses interrogations soulevant des problématiques concrètes rencontrées sur le terrain par les professionnels financiers. Cette dynamique interactive a non seulement démontré la pertinence du sujet, mais a également souligné le besoin croissant de partage de bonnes pratiques entre les secteurs privé et public pour renforcer l'efficacité de la lutte LBC/FT.

- Une deuxième édition de l'atelier a eu lieu le 9 décembre 2025 et s'est orientée vers les professions non financières, en réunissant le secteur des professions comptables et fiscales. Les discussions ont notamment porté sur plusieurs thèmes essentiels comme la protection du déclarant et l'utilité de la déclaration dans le système LBC/FT, les typologies et risques rencontrés par le secteur ainsi que la qualité des informations fournies sur goAML et les étapes à respecter après la déclaration.

Cette édition a suscité un vif intérêt, marqué par des échanges de grande qualité. Les nombreuses questions des participants ont enrichi le débat et renforcé la coopération entre la CTIF et les professionnels, optimisant ainsi l'efficacité du processus préventif. Ces réflexions partagées ont d'ailleurs nourri un article commun publié dans la revue de l'ITAA[29].

[29] https://www.itaa.be/books/itaa-zine_2026-01_fr-2/

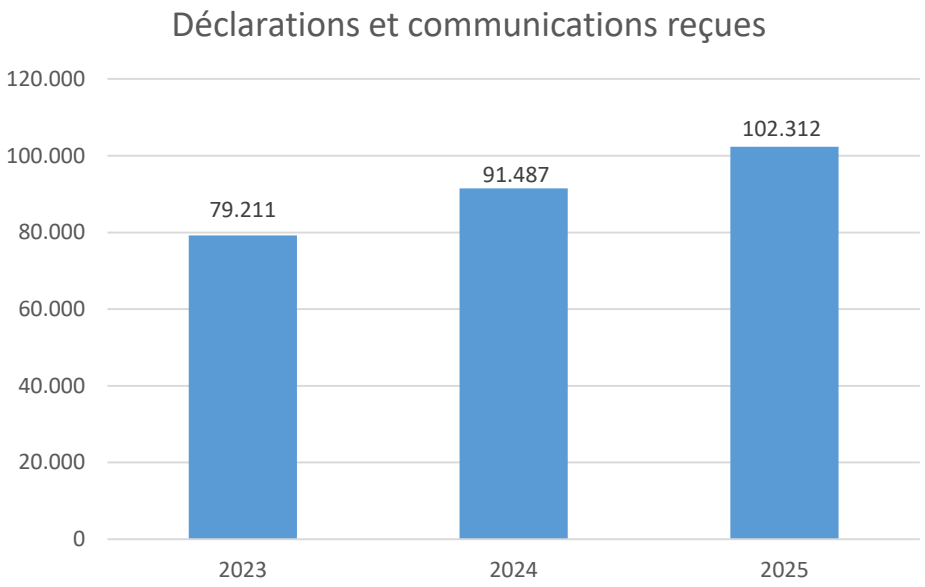
V. SYSTEME D'INFORMATION

1. Chiffres clés

1.1 Déclarations à la CTIF

En 2025, la CTIF a reçu un total de 102.312 déclarations de soupçon ou communications d'informations.

	2023	2024	2025
Nombre total	79.211	91.487	102.312



Ces déclarations sont ventilées au point 2 ci-dessous par catégories d'entités assujetties.

1.2. Transmissions aux autorités judiciaires

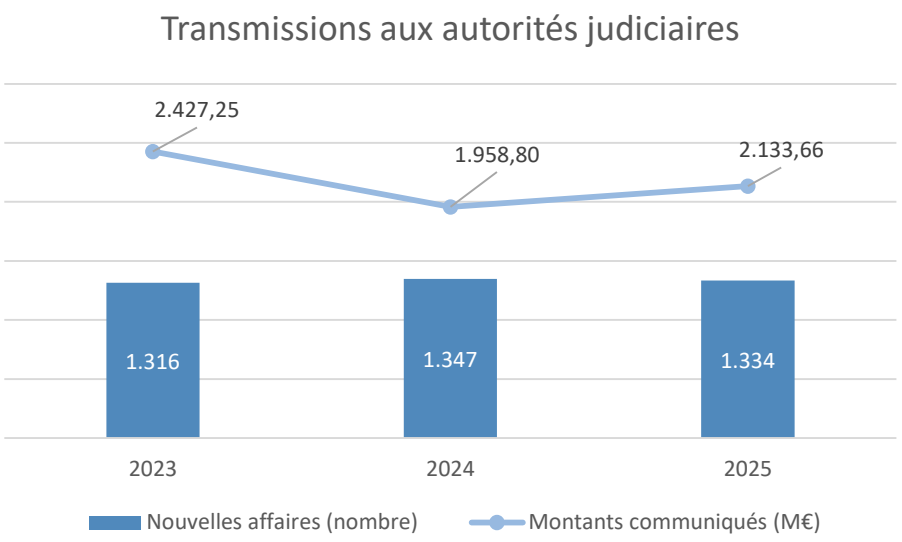
Lorsque la CTIF dispose d'indices sérieux de blanchiment de capitaux, de financement du terrorisme ou de financement de la prolifération des armes de destruction massive, elle transmet les résultats de son analyse au procureur du Roi ou au procureur fédéral. De plus, si des éléments complémentaires d'informations (de nouvelles transactions ou de nouveaux faits) sont par la suite portés à sa connaissance, elle en informe le procureur du Roi ou le procureur fédéral.

En 2025, la CTIF a transmis 1.334 nouveaux dossiers aux autorités judiciaires pour un montant total de 2,13 milliard EUR.

En vertu de la loi du 18 septembre 2017, la CTIF transmet également une copie de son rapport d'analyse à l'auditeur du travail lorsque la transmission au procureur du Roi ou au procureur fédéral concerne des informations relatives aux blanchiment de capitaux provenant du trafic d'êtres humains, de la traite des êtres humains ou de la fraude sociale[30].

[30] Article 83 de la loi du 18 septembre 2017.

	2023	2024	2025
Procureur du Roi ou procureur fédéral			
Nouvelles affaires (nombre)	1.316	1.347	1.334
Montants communiqués (M€)	2.427,25	1.958,80	2.133,66
Nombre de copies à l'Auditeur du travail	607	617	760



Lorsqu'un dossier est transmis aux autorités judiciaires, la CTIF, communique également, dans un certain nombre de cas et en vertu de la loi du 18 septembre 2017, des informations utiles issues de ses rapports de transmission (ou une copie du rapport) aux autorités administratives énumérées à l'article 83 de cette loi (cfr. 4.2).

1.3. Oppositions de la CTIF

La loi du 18 septembre 2017 (art. 80) permet à la CTIF, lorsqu'elle est saisie d'une déclaration de soupçon ou d'informations en application de l'article 79 de la loi (y compris donc dans le cadre d'une demande d'assistance émanant d'une CRF étrangère), de s'opposer à l'exécution d'une transaction annoncée par une entité assujettie, mais aussi à l'exécution de toute opération qui y est afférente. La CTIF détermine les opérations et les comptes concernés par cette mesure.

En 2025, la CTIF s'est opposée à 259 reprises à l'exécution d'une opération pour un montant total de 15,36 millions EUR.

	2023	2024	2025
Nombre d'oppositions	62	110	259
Montant total des oppositions (M€)	4,49	9,63	15,36

Pour rappel, la CTIF avise aussi l'Organe Central pour la Saisie et la Confiscation lorsque, dans un dossier qu'elle transmet aux autorités judiciaires, des sommes ou des avoirs pour des montants significatifs sont disponibles en vue d'une saisie judiciaire (cfr. 4.2).

2. Activité déclarative

2.1. Déclarations

	2023	2024	2025	2025%
Etablissements de paiement	25.141	41.956	51.744	50,6%
Etablissements de crédit	40.129	39.642	39.654	38,8%
Etablissements de monnaie électronique	5.442	2.737	3.883	3,8%
Entreprises d'assurance-vie	2.374	1.242	1.396	1,4%
Notaires	1.150	824	832	0,8%
Sociétés de crédit hypothécaire	699	821	625	0,6%
Etablissements de jeux de hasard	322	173	530	0,5%
Professions comptables et fiscales	317	344	407	0,4%
Banque Nationale de Belgique	462	492	354	0,3%
Sociétés de crédit à la consommation	244	207	314	0,3%
Société de droit public bpost	643	632	196	0,2%
Sociétés de bourse	91	110	166	0,2%
Sociétés de location-financement	44	44	71	0,07%
Réviseurs d'entreprises	88	69	67	0,07%
Bureaux de change	44	38	59	0,06%
Agents immobiliers	39	31	22	0,02%
Entreprises d'investissement	23	16	20	0,02%
Huissiers de justice	21	21	19	0,02%
Prestataires de services aux sociétés	21	14	12	0,01%
Clubs de football professionnels de haut niveau	12	9	10	0,01%
Loueurs de coffre-fort	-	-	9	0,01%
Avocats	14	14	6	0,01%
Intermédiaires d'assurances	3	5	5	<0,01%
Marchands d'art	-	4	5	<0,01%
Sociétés de gestion d'organismes de placement collectif	-	2	3	<0,01%
Fédération royale belge de football	26	7	1	<0,01%
Commerçants en diamants	2	1	2	<0,01%
Courtiers en services bancaires et d'investissement	2	2	-	-
Prestataires de services d'échange entre monnaies virtuelles et monnaies légales	7	-	-	-
Géomètre-Expert	2	-	-	-
Entreprises de gardiennage	1	-	-	-
Total	*77.363*	*89.457*	*100.412*	*98,1%*

2.2. Demandes de renseignements et communications spontanées reçues des autres cellules de renseignement financier (homologues étrangers de la CTIF)

	2023	2024	2025	2025%
Cellules étrangères	1.173	1.105	1.472	1,4%

2.3. Communications à la CTIF par d'autres autorités compétentes

	2023	2024	2025	2025%
Service décisions anticipées en matière fiscale(1)	298	710	163	0,2%
SPF Finances	47	38	70	0,1%
Douanes et Accises(2)	42	12	25	0,02%
SPF Economie	11	10	5	<0,01%
Curateurs de faillite et administrateurs provisoires	4	3	5	<0,01%
Europol	5	4	3	<0,01%
Sûreté de l'Etat[31]	3	4	1	<0,01%
Centre d'Information et d'avis sur les organisations sectaires	1	3	1	<0,01%
Etablissements pénitenciers	3	3	-	-
Service Général du Renseignement et de la Sécurité[32]	2	2	-	-
SPF Affaires étrangères	-	-	-	-
Organe de Coordination pour l'Analyse de la Menace[33]	1	-	-	-
Vlaamse Belastingdienst(1)	2	1	-	-
Total	*419*	*790*	*273*	*0,3%*

(1) Comprend les attestations de régularisations fiscales communiquées à la CTIF par ce service.

(2) Comprend les déclarations de transport transfrontalier d'argent liquide en application du Règlement (CE) n°1889/2005 du 26 octobre 2005 et à partir du 2 juin 2021 du Règlement (UE) 2018/1672 du Parlement européen et du Conseil du 23 octobre 2018 relatif aux contrôles de l'argent liquide entrant dans l'Union ou sortant de l'Union et abrogeant le règlement (CE) n°1889/2005 et de l'AR du 26 janvier 2014 portant certaines mesures relatives au contrôle du transport transfrontalier d'argent liquide.

En 2021, la Commission européenne a développé une application informatique permettant aux Douanes de communiquer de manière centralisée les déclarations de transport transfrontalier d'argent liquide dans une base de données commune que les CRF peuvent consulter. La diminution du nombre de communications par les Douanes et Accises au cours des dernières années est donc purement technique.

[31] VSSE
[32] SGRS
[33] OCAM

2.4. Communications à la CTIF par les autorités de contrôle, de tutelle ou disciplinaires

	2023	2024	2025	2025%
FSMA[34]	177	98	19	0,02%
ITAA[35]	79	31	136	0,1%
SPF Economie - Service des Licences (Diamant)	-	4	-	-
Collège de Supervision des Réviseurs d'entreprises	-	2	-	-
Total	*256*	*135*	*155*	*0,2%*

TOTAL GENERAL (2.1 - 2.4)	79.211	91.487	102.312	100%

Le secteur des établissements de paiement

L'augmentation du nombre total de déclarations reçues est principalement due à la forte croissance observée dans le secteur des établissements de paiement avec près de 52.000 déclarations émanant en 2025 de ce secteur, soit une augmentation de près de 10.000 déclarations en une année. Néanmoins, cette hausse de l'activité déclarative doit être correctement interprétée étant donné que certains de ces établissements proposent leurs services de paiement depuis la Belgique à des clients dans plusieurs pays de l'UE, grâce au passeport européen. Plus de 90% de ces déclarations sont, après un examen par la CTIF, externalisées vers ses homologues européens dans le cadre du processus « *cross border reporting* » vu l'absence de lien direct avec notre pays. Malgré cette externalisation, les informations issues des déclarations des établissements de paiement permettent néanmoins de constituer un socle important d'informations pour la CTIF.

[34] Autorité des Services et Marchés Financiers
[35] Institute for Tax Advisors and Accountants

3. Coopération internationale

Cette année encore, la CTIF a adressé de nombreuses demandes de renseignements à l'étranger et en a également reçu un grand nombre de la part de ses homologues de pays européens ou de pays tiers. Les données statistiques concernant la coopération internationale figurent ci-dessous.

L'échange d'informations s'opère toujours de manière protégée. Les données échangées ne peuvent être utilisées sans l'autorisation préalable de la cellule de renseignement financier concernée et ne le sont qu'à titre de renseignement.

La CTIF attache une grande importance à la protection des données qu'elle communique à des cellules de renseignement financier étrangères.

Lorsque la CTIF est saisie d'une déclaration de soupçon qui concerne un autre pays de l'UE, elle externalise de manière automatique et standardisée les données de cette déclaration à ses homologues étrangers concernés, en vertu de la loi du 18 septembre 2017. Des informations détaillées sur ce mécanisme d'externalisation se trouvent au point 4.4 ci-après.

Les chiffres repris ci-dessous, relatifs aux demandes de renseignements reçues (1.472) et envoyées (2.227), comprennent non seulement les demandes courantes de renseignements, mais aussi les échanges spontanés de renseignements. Il est question d'échange spontané de renseignements lorsque la CTIF informe, par exemple, un homologue étranger de la transmission d'un dossier et que des liens ont pu être établis avec le pays de cet homologue étranger, même si la CTIF n'a pas préalablement adressé de demande de renseignements à cet homologue. Inversement, la CTIF reçoit parfois d'homologues étrangers, par exemple, des renseignements au sujet de ressortissants belges victimes d'une escroquerie dans le pays de l'homologue étranger ou des avertissements[36] relatifs à certaines formes d'escroquerie. De tels échanges d'informations sont également considérés par la CTIF comme des échanges spontanés de renseignements.

	Coopération internationale entrante (demandes et communications reçues par la CTIF)			Coopération internationale sortante (demandes et communications envoyées par la CTIF)		
Région[37]	Demandes de renseignements	Communications spontanées	Total	Demandes de renseignements	Communications spontanées	Total
Europe	818	472	**1290**	391	1612	**2003**
Amérique du Nord et du Sud	15	114	**129**	14	61	**75**
Moyen-Orient et Afrique du Nord	21	7	**28**	7	64	**71**
Asie et Pacifique	6	7	**13**	8	63	**71**
Afrique	8	0	**8**	3	3	**6**
Eurasie	4	0	**4**	1	0	**1**
Total	**872**	**600**	**1.472**	**424**	**1.803**	**2.227**

Outre les communications spontanées dans le cadre de dossiers individuels, la CTIF a également envoyé en 2025 des communications spontanées portant sur des thèmes plus transversaux, tels que l'utilisation de la technique de la compensation, du blanchiment basé sur le commerce (TBML) et des

[36] La communication d'avertissements au sujet de techniques de blanchiment se fait via le site internet ou le rapport annuel de la CTIF.
[37] Les homologues sont classés dans ce tableau suivant leur appartenance aux sous-groupes du Groupe Egmont et du GAFI (FSRB's).

paiements effectués pour compte de tiers (TPP) et le transport transfrontalier d'argent liquide. Ces échanges ne figurent pas dans le tableau ci-dessus.

Parmi les communications spontanées sortantes, on trouve 1.528 communications effectuées dans le cadre d'opérations de type *Correspondent Banking*.

Le Correspondent Banking représente la fourniture de services bancaires[38] par une banque (la « banque correspondante ») à une autre banque (la « banque cliente »). Les grandes banques internationales agissent généralement comme correspondants pour des milliers d'autres banques à travers le monde. Les banques clientes peuvent bénéficier d'un large éventail de services, y compris la gestion de la trésorerie (par exemple, les comptes porteurs d'intérêts dans une variété de devises), les virements internationaux, la compensation des chèques, les comptes créditeurs et les services de change.

Les services de Correspondent Banking englobent une série de services qui ne comportent pas tous le même niveau de risque BC/FT. Certains de ces services bancaires présentent un risque BC/FT plus élevé car l'établissement correspondant traite ou exécute des transactions pour les clients de ses clients.

Enfin, à titre complémentaire à la procédure d'échange spontané, la CTIF utilise également la procédure XBD « Cross-border dissemination[39] » qui concerne la réception d'une déclaration 'classique' pouvant présenter un intérêt pour une ou plusieurs autres CRF européennes et dont des informations sont transmises à nos homologues européens, avant toute analyse.

[38] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Correspondent-banking-services.html
[39] Voir page 47 - Dissémination aux cellules de renseignement financier européennes

4. Dissémination de l'information

4.1. Transmission aux autorités judiciaires

En 2025, la CTIF a transmis 1.334 nouveaux dossiers aux autorités judiciaires pour un montant total de 2,13 milliard EUR.

Si de nouvelles déclarations de soupçon sont adressées à la CTIF concernant des transactions en rapport avec la même affaire (déclarations complémentaires) et si des indices sérieux de blanchiment de capitaux ou de financement du terrorisme sont toujours présents, la CTIF communique sous forme de rapport complémentaire les nouvelles opérations suspectes.

Ces rapports complémentaires transmis aux autorités judiciaires portent sur un montant total de 383,09 millions EUR en 2025.

A 760 reprises, une copie du rapport d'enquête a été transmise en parallèle à l'auditeur du travail en application de l'article 83 de la loi du 18 septembre 2017.

La CTIF partage également comme prévu par la loi des informations spécifiques avec plusieurs autorités administratives (cfr. 4.2.).

En l'absence d'indices sérieux de blanchiment ou de financement du terrorisme, la CTIF n'effectue aucune communication aux autorités judiciaires, mais les informations issues des déclarations de soupçon ne sont pas perdues pour autant.

Même si un dossier n'est pas transmis aux autorités judiciaires, les informations qu'il contient peuvent être transmises par la CTIF aux services de renseignements et à l'OCAM dans le cadre de la lutte contre le processus de radicalisation, le terrorisme, son financement et les activités de blanchiment qui pourraient y être liées (cfr. 4.2.).

La CTIF communique aussi beaucoup avec ses homologues étrangers, plus particulièrement lorsque les déclarations émanent d'entités assujetties actives depuis la Belgique sous le régime de la libre prestation de services (cfr. 4.4.).

4.2. Dissémination aux autorités administratives

Les membres de la CTIF et les membres de son personnel sont soumis à un secret professionnel strict.

Cependant, ce secret professionnel est levé dans un certain nombre de cas énumérés de manière limitative à l'article 83 de la loi du 18 septembre 2017, ce qui a permis à la CTIF d'échanger et de communiquer des informations utiles aux services/autorités repris ci-dessous :

Art. 83 de la loi du 18 septembre 2017 - nombre de communications	2023	2024	2025
Service de Coordination Anti-Fraude (CAF)	675	700	792
Service d'Information et de Recherche Sociale (SIRS)	583	471	594
Organe Central pour la Saisie et la Confiscation (OCSC)	68	110	259
Douanes et Accises	23	13	32
Organe de Coordination pour l'Analyse de la Menace (OCAM)	51	35	26
Sûreté de l'Etat (VSSE)	51	35	26
Service Général du Renseignement et de la Sécurité (SGRS)	51	35	26

SPF Economie	20	15	15
FSMA	6	9	9
Trésorerie[40]	4	3	6
Banque de données commune T.E.R.[41]	11	13	6
Office européen de lutte antifraude (OLAF)[42]	3	1	5

4.3. Echanges avec les autorités de contrôle et les déclarants

Coopération et échanges d'informations avec les autorités de contrôle

En application de l'article 121 de la loi du 18 septembre 2017, la coopération entre la CTIF et les autorités de contrôle s'est poursuivie tout au long de l'année 2025 via des échanges d'informations effectués d'initiative ou sur demande ainsi que par l'organisation de réunions de concertation périodiques en vue de partager les expertises respectives susceptibles d'être utiles à l'autre service.

Pour rappel, les communications de la CTIF vers les autorités de supervision se répartissent en trois catégories principales :

- les retours d'informations sur l'activité déclarative des entités soumises à leur contrôle (quantité et qualité des déclarations reçues) ;
- les signalements relatifs à d'éventuels manquements aux obligations prévues par la loi LBC/FT (dont obligation de vigilance à l'égard des clients et des opérations et obligation de déclaration) ;
- les transmissions d'informations spécifiques liées à un dossier dénoncé au parquet impliquant une entité sous leur supervision.

Cette coopération permet de renforcer l'efficacité des contrôles et d'améliorer la conformité du secteur financier et non financier face aux obligations LBC/FT.

De son côté, la CTIF est informée par les autorités de contrôle des principales informations suivantes :

- les résultats des analyses individuelles de risques ;
- les faiblesses constatées lors d'un contrôle pouvant avoir un impact sur l'activité déclarative d'une entité assujettie ou sur l'analyse des opérations atypiques par celle-ci ;
- les actions de sensibilisation menées auprès des secteurs soumis à leur contrôle.

Celle-ci est d'ailleurs régulièrement amenée à participer de manière active aux sessions de sensibilisation organisées par les autorités de contrôle.

La CTIF assiste enfin, en tant qu'observatrice, aux divers collèges de supervision en matière de LBC/FT organisés par la BNB et concernant des institutions financières belges sous son contrôle qui ont des filiales, succursales ou autres formes d'établissement dans au moins deux autres Etats membres de l'UE. Un retour d'information sur l'activité déclarative de l'institution financière faisant l'objet du collège est néanmoins donné par la CTIF à cette occasion.

[40] Echanges entre la CTIF et l'Administration générale de la Trésorerie du SPF Finances, rendus faisables depuis le 10 décembre 2022, dans le cadre de la mise en œuvre des sanctions financières, embargos et mesures restrictives qui sont prises par les Nations Unies, l'Union européenne ou la Belgique vis-à-vis de pays, de personnes ou d'entités dans l'objectif de mettre fin aux violations de la paix et la sécurité internationales comme le terrorisme, les violations des droits de l'homme, la déstabilisation des Etats souverains et la prolifération d'armes de destruction massive.
[41] La Banque de données commune « Terrorisme, Extrémisme, Processus de Radicalisation » (BDC T.E.R.) contient les noms des personnes qui sont suivies de manière prioritaire dans le cadre de l'extrémisme ou du terrorisme dans notre pays.
[42] Accord de coopération signé en 2022 entre l'Office européen de lutte antifraude et la CTIF.

Retour d'informations vers les déclarants

Afin d'améliorer la qualité de l'activité déclarative, la CTIF a mis en place depuis de nombreuses années un dispositif de retour d'information vers les entités assujetties. Ce dispositif vise à améliorer leur compréhension des typologies de BC/FT, à affiner leurs mécanismes de détection des opérations suspectes et à les aider à effectuer des déclarations de qualité.

La CTIF veille à assurer un retour d'information à la fois sur le plan individuel et sectoriel, notamment au moyen des dispositifs suivants :

- la publication des rapports annuels sur le site internet de la CTIF ;
- les différents documents de soutien destinés aux déclarants sur le site internet de la CTIF dont les principaux sont :
    - le « Vademecum », qui présente un aperçu de diverses typologies constatées par la CTIF, avec d'une part un accent sur les techniques de blanchiment et d'autre part sur différents secteurs à risque[43] ;
    - les « Lignes directrices destinées aux entités assujetties », qui contiennent des informations importantes relatives au processus de déclaration[44] ;
    - les « Critères d'alerte » auxquels les déclarants doivent accorder une attention particulière concernant certains types d'opérations et certains secteurs de déclarants (critères d'alerte spécifiques applicables uniquement ou principalement à une catégorie professionnelle déterminée) [45] ;
    - la « Qualité des déclarations », un document qui donne un aperçu des éléments importants devant figurer dans une déclaration adressée à la CTIF[46].
- la participation aux sessions de sensibilisation organisées par les autorités de contrôle et certaines professions assujetties ;
- un retour d'information individuel aux déclarants concernant leur activité déclarative et la qualité de leurs déclarations, fourni de manière proactive à la suite de certains constats ou à la demande du déclarant lorsque cela s'avère nécessaire ;
- un nouveau format d'ateliers LBC/FT, dont deux éditions ont été organisées par la CTIF en 2025 dans le cadre d'un retour sectoriel destiné aux déclarants[47].

De l'importance de recevoir des déclarations de qualité

La CTIF attache une importance de plus en plus grande au fait de recevoir des déclarations de qualité car cela lui permet de procéder, dès le départ, à un filtrage correct et une orientation adéquate des déclarations dont le nombre ne cesse de croître d'année en année, et d'ainsi rendre ses analyses davantage performantes tant sur le plan opérationnel que sur le plan stratégique.

L'appréciation de la qualité des déclarations effectuée par la CTIF se base sur une analyse du caractère clair, précis et complet de celles-ci ainsi que d'un examen de la motivation du soupçon. Une attention particulière est également portée à la correcte structuration des données, d'autant que le nouvel outil de déclaration en ligne goAML prévoit de nouveaux formulaires web et des champs additionnels à remplir, et au délai dans lequel les déclarations sont effectuées.

[43] Lien vers Vademecum
[44] Lien vers Lignes directrices
[45] Lien vers Critères d'alerte
[46] Lien vers Qualité des déclarations
[47] Voir page 35 pour plus de détails.

D'une manière globale, les retours d'information sur la qualité des déclarations donnés aux déclarants au cours de ces dernières années ont permis de constater les principales améliorations suivantes :

- l'identité des mandataires/bénéficiaires effectifs est reprise de manière plus systématique dans les déclarations, ce qui permet à la CTIF de faire directement les liens utiles avec des intervenants qui seraient déjà connus de celle-ci ;

- en cas de déclarations groupées relatives à une série d'intervenants, les liens existant entre ceux-ci sont clairement expliqués de manière plus régulière, ce qui permet à la CTIF de mieux cerner le principal intervenant sur lequel centrer son analyse. Ceci lui évite de devoir retourner vers le déclarant afin d'obtenir les éclaircissements utiles ou alors de devoir scinder la déclaration par intervenant, ce qui entraîne une surcharge de travail administratif.

- le volume global des opérations suspectes et la période de celles-ci sont plus fréquemment mentionnés dans les déclarations, ce qui permet à la CTIF de mieux filtrer et orienter les déclarations ;

- il n'y a plus aucune déclaration faisant simplement référence à des transferts internationaux sans qu'aucune indication ne soit donnée sur l'origine et/ou la destination des fonds ;

- il est plus souvent fait explicitement référence au fait que le client a été interrogé sur les opérations et que celui-ci n'a, le cas échéant, pas souhaité répondre ou a donné des réponses non satisfaisantes, ce qui permet à la CTIF de s'assurer de la pertinence d'indicateurs tels que « origine des fonds pas connue » ou « transparence fiscale des fonds non vérifiée» ;

- le recours à des déclarations mécaniques fondées exclusivement sur des critères objectifs et automatiques (tels que des dépassements de seuils), sans qu'aucun élément d'analyse ne vienne étayer le soupçon, tend à diminuer ;

- les déclarations de type *correspondent banking* sont davantage motivées par des indicateurs variés et ne sont plus uniquement basées sur des informations négatives récoltées de sources ouvertes ;

- les déclarations consécutives à un réquisitoire judiciaire sont désormais plus souvent motivées par l'identification d'opérations suspectes issues d'une analyse et ne se limitent plus à la seule référence au réquisitoire.

4.4. Dissémination aux cellules de renseignement financier européennes

L'article 53.1 de la 4ème Directive LBC/FT Européenne impose aux Etats membres de coopérer de manière immédiate avec leurs homologues étrangers de l'UE: « When an FIU receives an STR which concerns another Member State, it shall promptly forward it to the FIU of that Member State ».

Cette disposition a été transposée dans la loi du 18 septembre 2017 à l'article 124 qui précise que : « Lorsque la CTIF est saisie d'une déclaration de soupçon, établie par une entité assujettie en application des articles 47 ou 54, qui concerne un autre pays, elle transmet à la CRF du pays concerné connecté à FIU.Net, dans les meilleurs délais, pour analyse, toutes les informations contenues dans la déclaration. »

On distingue plusieurs formes de coopération « cross-border », dont les XBD et XBR.

- XBR « *Cross-border reporting* »: réception d'une déclaration effectuée par un assujetti qui exerce une activité principale en libre prestation de services au départ de la Belgique et qui est donc soumis à la loi LBC/FT belge mais dont la grande majorité des déclarations ne concernent pas

ou n'ont aucun lien direct avec notre pays. Les personnes concernées n'ont aucun lien avec la Belgique. Les informations sont uniquement pertinentes pour un autre État membre. Dans ce cas, la CTIF communique l'entièreté du contenu de la déclaration de soupçon à la CRF/aux CRF concernée(s) pour qu'elle(s) l'analyse(nt) elle(s)-même(s).

> *Exemple opérationnel :*
>
> Un établissement de paiement établi en Belgique fournit des services de transfert de fonds à une personne physique résidante dans un État membre de l'Union européenne autre que la Belgique. Après avoir détecté des opérations suspectes impliquant ce client étranger, sans autre lien avec la Belgique que l'IBAN belge qui est mis à sa disposition, l'établissement de paiement effectue une déclaration de soupçon auprès de la CTIF. Dès réception, la CTIF transmet l'intégralité de la déclaration à la CRF du pays où la personne est localisée, via XBR, afin qu'elle puisse réaliser l'analyse opérationnelle.

- XBD « *Cross-border dissemination* »: réception d'une déclaration 'classique' pouvant présenter un intérêt pour une ou plusieurs autres CRF européennes. Au moins un des intervenants a un lien avec la Belgique, mais les informations sont également pertinentes pour un autre État membre. La transmission des informations à la/aux CRF concernée(s) se fera sous forme de « metadata » et de manière « promptly » et donc dès la réception de la déclaration, avant toute analyse.

> *Exemple opérationnel :*
>
> Un établissement de paiement établi en Belgique détecte des opérations suspectes impliquant un client résidant en Belgique, victime d'une fraude, qui a transféré des fonds vers un compte bancaire détenu par une mule financière ou un escroc établi dans un autre État membre de l'Union européenne. A la suite de cette détection, l'établissement de paiement effectue une déclaration de soupçon auprès de la CTIF.
>
> Dans ce cas présent, et avant même l'analyse approfondie de la déclaration, la CTIF va rapidement transmettre à l'Etat membre impliqué, via XBD, certaines informations essentielles relatives au dossier (« metadata »), telles que les références du compte bancaire ou des transactions, l'identité de la personne impliquée et certains éléments contextuels liés aux opérations suspectes.

La procédure XBD ne remplace ainsi pas la procédure d'échange spontané qui s'effectue plus en cours ou en fin d'analyse du dossier. Les deux procédures sont à ce titre complémentaires, un XBD initial (ou l'absence d'un XBD) n'excluant pas un échange spontané ultérieur.

Nombre de	2023	2024	2025
XBR	19.574	35.455	47.533
XBD	193	329	113

La CTIF répond également à des demandes de renseignements de cellules de renseignement financier étrangères et communique à celles-ci des informations déjà en sa possession ou qu'elle a récoltées auprès des entités assujetties, services de police et autres autorités administratives en Belgique.

5. Chiffres et précisions complémentaires

5.1. Transmissions par type de déclarants

L'utilisation du nouveau système de déclarations en ligne goAML depuis la fin de l'année 2024 s'est accompagnée d'une nouvelle approche en termes de comptabilisation des communications (déclarations d'opérations, de fonds ou de faits suspects, et informations des homologues étrangers et services de l'Etat) utilisées au sein des nouveaux dossiers transmis aux autorités judiciaires. Etant donné qu'une nouvelle affaire transmise aux autorités judiciaires est le fruit d'une analyse qui peut reposer sur un ensemble de déclarations de soupçon ou communications d'informations, il est important que les statistiques relatives à la répartition du nombre de nouvelles affaires transmises aux autorités judiciaires par type de déclarants ne se limite pas à une seule source d'information qualifiée comme principale.

Le tableau suivant propose une répartition du nombre de déclarations de soupçon ou communications d'information, par type de déclarants, qui ont été utilisés à des fins de transmission aux autorités judiciaires, dans le cadre d'une nouvelle affaire (1) ou lors d'une transmission complémentaire (2), indépendamment des autres mécanismes de dissémination de l'information aux niveaux national et international.

	2025(1)	2025%(1)	2025(2)
Etablissements de crédit	1.789	85,8%	572
Cellules étrangères	117	5,6%	31
Etablissements de paiement	90	4,3%	21
SPF Finances	25	1,2%	4
Etablissements de jeux de hasard	13	0,6%	2
Etablissements de monnaie électronique	11	0,5%	2
Professions comptables et fiscales	8	0,4%	2
Notaires	6	0,3%	3
FSMA	4	0,2%	-
Sociétés de crédit à la consommation	4	0,2%	2
Société de droit public bpost	3	0,1%	3
Banque Nationale de Belgique	3	0,1%	1
Bureaux de change	2	0,1%	-
Service décisions anticipées en matière fiscale	2	0,1%	-
Intermédiaires d'assurances	1	0,05%	-
Loueurs de coffre-fort	1	0,05%	-
Prestataires de services aux sociétés	1	0,05%	-
Service Général du Renseignement et de la Sécurité	1	0,05%	-
Sociétés de bourse	1	0,05%	-
Sociétés de gestion d'organismes de placement collectif	1	0,05%	-
Sociétés de location-financement	1	0,05%	-
Entreprises d'assurance-vie	1	0,05%	5
Réviseurs d'entreprises	-	-	2
SPF Economie	-	-	1
Total	*2.085*	*100%*	*651*

5.2. Criminalités et circonstances sous-jacentes

Criminalités et circonstances sous-jacentes	2023(1)	2023(2)	2024(1)	2024(2)	2025(1)	2025(2)
Escroquerie	341	53,35	304	141,77	289	422,85
Phénomène des blanchisseurs professionnels[48]	191	683,89	215	626,82	272	688,04
Fraude sociale	184	151,73	168	168,20	250	153,91
Fraude fiscale grave	194	1158,46	165	642,84	114	465,54
Trafic illicite de stupéfiants et de substances psychotropes	123	25,60	151	11,40	106	18,45
Criminalité informatique	2	3,08	14	0,01	61	11,78
Criminalité organisée	88	146,23	85	175,72	50	227,43
Trafic illicite d'armes, de biens et de marchandises	32	59,62	38	83,59	43	20,70
Abus de biens sociaux	34	25,29	50	21,88	36	14,68
Abus de confiance	22	6,26	12	12,07	26	8,06
Infraction liée à l'état de faillite	37	22,39	43	8,73	21	5,09
Détournement et corruption	9	12,55	15	29,52	16	26,85
Exploitation de la prostitution	17	4,87	23	3,37	14	8,58
Terrorisme, financement du terrorisme et financement de la prolifération	12	0,50	10	6,87	11	0,93
Trafic d'êtres humains	4	3,12	8	4,77	4	6,86
Vol ou extorsion	8	0,51	7	0,90	5	0,77
Criminalité environnementale grave	-	-	1	0,36	3	37,44
Traite des êtres humains	11	68,37	7	2,66	5	0,43
Autres	7	1,41	31	17,34	8	15,27
Total	*1.316*	*2.427,25*	*1.347*	*1.958,80*	*1.334*	*2.133,66*

(1) Répartition du nombre de nouvelles affaires transmises aux autorités judiciaires par type de criminalités et circonstances sous-jacentes
(2) Répartition du montant (M€) communiqué aux autorités judiciaires par type de criminalités et circonstances sous-jacentes au sein des nouvelles affaires

Ainsi, sur les 1.334 nouveaux dossiers transmis aux autorités judiciaires en 2025, des informations provenant de 2.085 déclarations de soupçon ou communications ont été utilisées.

Les montants repris ci-dessus doivent être examinés et interprétés avec prudence. En fonction de la criminalité sous-jacente et de la technique de blanchiment utilisée, ils peuvent être à la fois constitués d'opérations de blanchiment et d'opérations commerciales réelles (c'est le cas en particulier dans les dossiers en rapport avec la fraude à la TVA ou le trafic illicite de biens et de marchandises). Il est souvent difficile dans ce type de dossiers de distinguer avec précision la part qui correspond à des opérations de blanchiment de celle qui correspond à des opérations commerciales réelles, puisque le blanchiment consiste justement à mélanger les opérations de blanchiment avec des opérations commerciales parfaitement légales. Les montants renseignés dans le tableau ci-dessus pour la fraude fiscale et la fraude sociale ne doivent en aucun cas être interprétés comme représentant le montant total de la fraude (fiscale ou sociale) en Belgique en 2025 (c'est à dire les montants

[48] Voir notamment page 25 pour plus d'information au sujet du recours à des sociétés écrans de compensation.

réellement éludés à l'impôt). Les montants dans le tableau ci-dessus peuvent être à la fois des fonds liés à du blanchiment et des capitaux dissimulés à l'étranger et rapatriés. Par contre, pour d'autres criminalités (l'escroquerie, la corruption et le détournement par exemple), les montants qui sont renseignés correspondent beaucoup plus aux montants blanchis et issus de ces formes de criminalités car ils sont directement et généralement exclusivement issus de l'activité criminelle sous-jacente.

Dans un même dossier, la CTIF peut arriver à la conclusion sur la base de son analyse qu'il existe des indices sérieux de blanchiment de capitaux en relation avec une ou plusieurs criminalités sous-jacentes. Il faut rappeler que la CTIF n'a pas les mêmes pouvoirs d'enquête que les autorités judiciaires et les services de police et travaille à partir d'indices et non pas de preuves.

VI. LEXIQUE

Informal Value Transfer System (IVTS) : Un système informel de transfert de valeur désigne tout système, mécanisme ou réseau de personnes qui reçoit de l'argent dans le but de transférer les fonds ou une valeur équivalente à un tiers situé dans un autre lieu géographique, sous la même forme ou sous une forme différente. Les transferts s'effectuent généralement en dehors du système bancaire formel, par l'intermédiaire d'institutions financières non bancaires ou d'autres entités commerciales dont l'activité principale n'est pas le transfert de fonds.

Payment Service Provider (PSP) **:** Prestataire de services de paiement qui organise, vérifie et autorise les paiements online.

Politically Exposed Persons (PEP) : Personne physique qui occupe ou a occupé une fonction publique importante.

Services Based Money Laundering (SBML) : Technique de blanchiment qui repose sur l'exploitation du commerce des services afin de dissimuler, convertir ou transférer des capitaux illicites.

Third Party Payments (TPP) : Paiements effectués par un tiers (third party) au nom ou pour le compte d'un payeur en faveur d'un bénéficiaire. Généralement, il s'agit de la livraison ou d'un service payé par un tiers qui n'est ni acheteur ni vendeur.

Trade Based Money Laundering (TBML) : Technique de blanchiment qui consiste à exploiter les transactions commerciales afin de dissimuler, convertir ou transférer des capitaux illicites.

Trade Based Terrorism Financing (TBTF) **:** Technique qui consiste à dissimuler le mouvement des fonds via l'utilisation de transactions commerciales dans le but de financer le terrorisme. Le TBTF utilise le même processus que le TBML, avec la différence que les fonds déplacés peuvent provenir à la fois de sources légitimes et illégitimes.

Underground Banking (UB) : Banque souterraine est un terme générique pour décrire des mécanismes utilisés pour contourner le secteur financier formel et transférer des fonds, parfois sans déplacement physique de l'argent.

Virtual Asset Service Provider (VASP) **:** Prestataire de services d'actifs virtuels.

CELLULE DE TRAITEMENT DES INFORMATIONS FINANCIERES
Rue de la Régence 52 - 1000 Bruxelles
Téléphone: 02/533.72.11
E-mail: info@ctif-cfi.be
Internet: www.ctif-cfi.be

Editeur responsable:
Philippe de KOSTER
Rue de la Régence 52 - 1000 Bruxelles

Toutes informations complémentaires et l'interprétation des chiffres et statistiques fournis dans le présent document peuvent être obtenues en adressant une demande écrite à l'adresse mail suivante : info@ctif-cfi.be

Couverture et illustrations aux pages 20, 23, 28 et 30 ont été créées par Magnific (www.magnific.com).