Cellule de Traitement des Informations Financières
Avenue de la Toison d'Or 55 boîte 1 – 1060 Bruxelles
Tél. : +32 2 533 72 11
Fax : +32 2 533 72 00
E-mail : info@ctif-cfi.be

Évolutions des tendances du blanchiment de capitaux
2023

1.1. Principales menaces

1.1.1. Le trafic de stupéfiants

Au niveau européen, la Belgique occupe une place centrale au sein du trafic de stupéfiants. Cette réalité n'a fait que se confirmer au cours de ces dernières années, des rapports d'organisations internationales tels que ceux publiés par l'Office des Nations Unies contre la drogue et le crime (ONUDC)[1] et l'Observatoire européen des drogues et des toxicomanies (OEDT)[2] mais aussi par la police fédérale[3] indiquant clairement que la Belgique est non seulement le principal point d'importation de la cocaïne en Europe, mais aussi un pays producteur et de transit pour les drogues de synthèse et le cannabis.

En outre, la violence associée à cette prééminence dans le trafic international devient de plus en plus visible. A Anvers, les organisations criminelles ne s'attaquent plus seulement entre elles, mais visent également les services publics en charge du transport et du stockage des cargaisons de cocaïne saisies. A Bruxelles, plusieurs règlements de compte mortels ont eu lieu en lien avec la lutte de territoires entre bandes rivales impliquées dans la vente locale, mais aussi dans la distribution en Europe.

Outre la violence, un autre effet pernicieux en lien avec le trafic de stupéfiants est le risque que les énormes profits issus de ce trafic très lucratif ne sapent l'économie légale. Comme contre-stratégie, les organisations criminelles essaient, en effet, de s'infiltrer dans le monde légal et tentent, via la corruption, d'avoir une emprise sur le tissu social et les structures politiques de notre société. Les enquêtes menées par la police à la suite du déchiffrage des systèmes de communication cryptés utilisés par les organisations criminelles ont donné une image inquiétante de la pénétration grandissante de ce monde criminel, souterrain, dans notre société.

L'une des initiatives visant à lutter contre cette infiltration est le projet de loi sur l'exécution administrative communale, approuvé au Parlement le 16 novembre 2023 et qui a abouti à la loi du 15 janvier 2024. Cette loi établit un cadre pour mieux armer les villes et les communes contre ces formes de criminalités, en élargissant les possibilités d'exécution préventive et répressive.

Au sein de l'opinion publique, il existe un appel croissant au développement, à moyen terme, d'une approche financière en matière de lutte contre les organisations criminelles impliquées dans le trafic de stupéfiants. Si cette approche « follow the money » convainc les forces de police, dans la pratique, elles sont parfois confrontées à un manque de moyens ou de profils spécialisés.

Pour les Cellules de renseignement financier (CRF) telles que la CTIF, l'approche financière du trafic de stupéfiants est une évidence. Le trafic de stupéfiants a, en effet, été la première forme de criminalité sous-jacente visée lors de la mise en place du dispositif préventif de lutte contre le blanchiment de capitaux à la fin des années 1980.

---

[1] World Drug report 2023 : https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html
[2] European Drug Report 2023 : Trends and Developments : https://www.emcdda.europa.eu/publications/european-drug-report/2023_en
[3] Rapport annuel de la police fédérale 2023 : https://www.police.be/rapportannuel-policefederale/fr/

Le défi pour la CTIF est d'analyser, le plus efficacement possible, les informations financières provenant des entités déclarantes en les liant aux informations policières, afin de pouvoir transmettre aux parquets, le plus rapidement possible, les informations les plus pertinentes et de compléter leurs enquêtes.

La coopération avec les services de police spécialisés dans la lutte contre le trafic de stupéfiants et la criminalité financière au sein de la direction centrale de la lutte contre la criminalité grave et organisée (DJSOC), la police judiciaire fédérale (PJF) et la police locale est donc très importante pour la CTIF. Par ailleurs, le Commissariat national « drogue », créé en 2023 et chargé de coordonner la lutte contre la criminalité liée à la drogue, est également un partenaire très précieux pour la CTIF.

Enfin, le trafic de stupéfiants et le blanchiment de capitaux qui en sont issus étant par excellence des phénomènes internationaux, l'importance de l'échange d'informations avec les CRF étrangères ne peut être sous-estimée.

L'analyse des dossiers liés au trafic de stupéfiants permet de distinguer deux catégories : l'auto-blanchiment et le blanchiment professionnel.

« Auto-blanchiment »

Dans ce premier type de dossier, les intervenants impliqués dans le trafic blanchissent eux-mêmes leurs revenus illicites. Il s'agit, en général, de dealers de niveau intermédiaire, de personnes qui gèrent des plantations de cannabis ou qui, d'une manière ou d'une autre, sont impliquées dans la récupération de la cocaïne contenue dans des conteneurs dans les ports. Cependant, dans un nombre très limité de cas, il a été constaté que des figures clés du trafic de cocaïne anversois avaient effectué des transactions financières en leur nom propre ou en utilisant des structures sociétaires, pour souscrire à des polices d'assurance-vie à l'étranger ou pour l'achat de crypto-monnaies.

En général, les montants figurant dans ces dossiers sont relativement limités, le montant moyen blanchi oscillant autour de 200.000 EUR par an. Souvent, les fonds sont déposés en espèces sur un compte bancaire, ce qui donne lieu à une analyse supplémentaire et à une communication finale à la CTIF. Il peut aussi bien s'agir de comptes personnels que de comptes professionnels liés à une société. Contrairement aux sociétés écrans utilisées par les réseaux professionnels de blanchiment, les sociétés figurant dans ce type de dossiers ont également une activité réelle et la personne impliquée dans le trafic de stupéfiants garde le contrôle de la société en tant que gérant - en son nom propre ou par l'intermédiaire de membres de sa famille.

Les secteurs d'activités les plus courants sont ***l'horeca, la vente au détail et la vente ou la location de voitures***. L'activité commerciale permet alors de déclarer une partie des dépôts en espèces comme chiffre d'affaires. L'exploitation d'un commerce peut aussi parfois être utilisée comme base ou point d'ancrage dans un quartier particulier, et sert alors à justifier d'un statut social plutôt qu'à blanchir de grandes sommes d'argent. Il ressort de certains dossiers, que des nightshops ou des bars à shisha sont utilisés comme point de rassemblement pour l'organisation criminelle ou servent même directement de point de distribution pour la drogue. L'application de la législation récente[4] par les administrations communales peut constituer une arme supplémentaire dans la lutte contre cette forme de blanchiment de capitaux.

Une autre technique couramment utilisée est celle du ***prêt d'argent*** de la part d'amis ou de la famille, le montant transféré sur le compte de l'emprunteur étant ensuite remboursé en espèces, via des versements échelonnés ou non. Inversement, des prêts peuvent également leur être accordés et les dépôts en espèces sont comptabilisés comme un remboursement de ces prêts.

Le secteur des ***voitures de luxe*** peut lui aussi être utilisé comme vecteur de blanchiment de capitaux par les trafiquants de stupéfiants. Il ressort de l'analyse des comptes bancaires, que les criminels, en tant que gérants de sociétés de vente ou de leasing de voitures, peuvent utiliser cette activité réelle pour mixer l'argent sale, provenant du trafic de stupéfiants, avec celui propre, provenant des activités réelles. Le criminel peut aussi, sans avoir aucun lien avec l'activité en tant que telle, effectuer des paiements importants pour des locations coûteuses de voitures de luxe auprès de sociétés de leasing belges, luxembourgeoises ou allemandes. Enfin, les voitures peuvent aussi être achetées, le montant transféré sur les comptes bancaires est alors bien inférieur à la valeur réelle du véhicule, de sorte que l'on peut soupçonner qu'une partie de l'achat a été payée autrement, vraisemblablement en espèces.

[4] Loi du 15 janvier 2024.

Les techniques de blanchiment des capitaux issus du trafic de stupéfiants peuvent également utiliser les investissements en matière de ***biens immobiliers***. Les revenus des trafics antérieurs peuvent être investis dans l'achat de biens immobiliers qui sont ensuite utilisés pour abriter des plantations de cannabis. Une autre variante consiste à réaliser une vente en-dessous du prix du marché pour des biens immobiliers qui nécessitent de lourds frais de rénovation. La rénovation se fait alors en grande partie « en noir », et est payée avec de l'argent du trafic. Lors de la revente, le montant total du bien provient de capitaux légalement acquis.

Notons enfin que ***les montres de luxe*** sont régulièrement utilisées comme vecteur pour le blanchiment de capitaux issus du trafic de stupéfiants. Les montres de luxe, de valeur stable et facilement transportables, peuvent être utilisées à la fois comme monnaie parallèle, pour déplacer leur valeur au-delà des frontières, ou comme investissements finaux pour des fonds criminels. Lors des perquisitions chez des membres d'une organisation criminelle active dans le milieu des stupéfiants, des montres de luxe y sont régulièrement saisies.

Réseaux professionnels de blanchiment

La grande majorité des revenus provenant du trafic de stupéfiants en Belgique sont acheminés vers des réseaux professionnels de blanchiment et ne sont donc pas blanchis par les trafiquants eux-mêmes. Ce deuxième type de dossiers porte sur des montants de plusieurs millions d'euros en quelques mois, circulant à travers un réseau de ***sociétés écrans***. La CTIF transmet ces dossiers au parquet dans le cadre de la criminalité organisée.

A l'instar de ce qu'il se passe au sein de l'économie légale, certaines prestations de services spécialisés commerciaux sont externalisées, les organisations criminelles faisant de plus en plus appel à des professionnels pour blanchir les revenus issus du trafic de stupéfiants, mais aussi d'autres formes de criminalités. Ces réseaux polycriminels opèrent à l'échelle internationale et utilisent des techniques telles que la 'compensation'[5], le 'blanchiment d'argent basé sur le commerce (TBML)'[6] et les 'paiements pour compte de tiers' (*voir infra*)[7] pour dissimuler la traçabilité des flux financiers. Le plus grand défi pour la CTIF est d'établir le lien entre le trafic de stupéfiants ou les personnes impliquées dans ce trafic et ces réseaux. Comme l'essentiel de l'argent est introduit en espèces, compte tenu du caractère international et du grand nombre de sociétés utilisées, il est souvent difficile d'en identifier l'origine exacte. L'interception des communications sécurisées des organisations criminelles montre d'ailleurs clairement le lien entre le trafic de stupéfiants et les réseaux professionnels de blanchiment, bien que ce lien ne soit pas toujours reflété dans les transactions financières.

La raison en est que les organisations criminelles utilisent des ***banques souterraines*** pour déplacer l'argent sale et l'introduire dans le réseau de blanchiment. Il s'agit d'un système bancaire clandestin qui fonctionne en dehors du système financier légal et qui permet de transférer de grandes quantités d'argent criminel à l'échelle internationale. Ce système est similaire à d'autres formes de transfert informel de fonds, comme le hawala, mais n'est utilisé que dans un contexte criminel.

Le travail de renseignement effectué par Europol après le démantèlement récent de trois outils de communication cryptée utilisés par des criminels a d'ailleurs révélé l'importance des banquiers clandestins dans le paysage criminel, qui opéraient jusqu'alors le plus souvent sous le radar des services répressifs. Dans ce contexte, Europol a mis en place la Taskforce opérationnelle TOKEN pour cibler les réseaux facilitant les opérations bancaires clandestines dans le monde entier[8].

La CTIF continuera de mettre l'accent sur la lutte contre ces réseaux professionnels responsables, entre autres, du blanchiment de sommes très importantes liées au trafic de stupéfiants.

---

[5] Le blanchiment par compensation désigne le processus qui permet aux criminels disposant d'espèces provenant de leurs activités illicites, de collaborer avec d'autres criminels qui ont un besoin de cash pour financer leurs activités illicites, afin que les espèces ne transitent pas par le système bancaire officiel. Les espèces remises de la main à la main sont compensées par des transferts bancaires sur des comptes souvent à l'étranger, sous couvert de fausses factures.

[6] Le blanchiment *basé sur le commerce ou le commerce de blanchiment d'argent* (TBML) désigne « le processus de dissimulation des gains criminels et de déplacement de la valeur en ayant recours à des transactions commerciales pour tenter de légitimer leur origine illégale ou de financer leurs activités », GAFI (2006), Blanchiment de *capitaux basé sur le commerce*.

[7] Paiements effectués par un tiers au nom ou pour le compte d'un payeur et en faveur d'un bénéficiaire.

[8] https://www.europol.europa.eu/media-press/newsroom/news/one-of-europe%E2%80%99s-biggest-underground-bankers-arrested-in-greece

1.1.2. La fraude fiscale grave

A l'instar de ces dernières années, le montant des dossiers transmis aux parquets en raison d'indices sérieux de blanchiment de capitaux provenant d'une fraude fiscale grave est particulièrement élevé. Le montant moyen par dossier dépasse plus de 5 millions d'euros et s'élève même à 50 millions d'euros dans plusieurs cas.

Ces montants élevés s'expliquent notamment par le fait que les flux financiers suspects identifiés dans les dossiers couvrent souvent une période de plusieurs années. C'est le cas, par exemple, des dossiers dans lesquels une grande quantité d'argent est rapatriée de l'étranger après que le capital a été accumulé pendant des années. La circulaire de la Banque nationale de Belgique du 8 juin 2021, dans laquelle la BNB invite les banques à faire preuve de la vigilance nécessaire lors du ***rapatriement de fonds*** de l'étranger non régularisés ou de manière incomplète, est toujours à l'origine de nombreuses déclarations à la CTIF.

Plusieurs dossiers traités par la CTIF en 2023 concernaient également des familles très fortunées ayant rapatrié des fonds pour lesquels il est apparu qu'ils étaient probablement entachés par d'importantes latences fiscales.
L'exercice de '*lookback'* imposé par la BNB semble toutefois se clôturer. Cette fin d'année 2023 a également été marquée par la fin de la procédure DLU quater. La CTIF sera particulièrement attentive aux potentielles conséquences au niveau de l'activité déclarative.

L'importance des montants peut également être expliquée par le secteur dans lequel les sociétés concernées opèrent. En 2023, plusieurs dossiers concernant des sociétés actives dans le ***secteur du diamant*** ont été signalés. Même si le nombre de dossiers est relativement limité, les montants en jeu dans le commerce des diamants sont si importants qu'ils pèsent lourdement dans les statistiques générales de la fraude fiscale.

Les parties impliquées dans ces dossiers utilisent souvent des structures internationales de sociétés affiliées qui leur permettent de manipuler le chiffre d'affaires et les bénéfices par le biais d'importations et d'exportations mutuelles de diamants commettant ainsi une fraude fiscale grave.

Les dossiers de « réserve quant à la valeur annoncée » du SPF Economie constituent un élément important pour détecter cette fraude. En collaboration avec les douanes, celui-ci contrôle chaque envoi entrant/sortant (en dehors de l'UE) et établit un dossier « réserve quant à la valeur annoncée» en cas de valeur différente sur la facture. Une bonne coopération avec nos partenaires du SPF Économie et du SPF Finances est donc cruciale.

Enfin, en 2023, la CTIF a traité plusieurs dossiers dans lesquels la fraude fiscale grave pouvait s'inscrire dans le cadre d'un réseau de sociétés (écrans) mis en place par des blanchisseurs professionnels. La fraude fiscale grave est alors combinée avec le blanchiment de capitaux provenant d'autres infractions sous-jacentes.

Dans ce type de dossiers, une attention particulière est attachée à la détection d'actifs potentiellement saisissables. A de nombreuses reprises, la CTIF a ainsi détecté des avoirs et fait usage de la possibilité qui lui est offerte de faire opposition à l'exécution d'opérations, ouvrant ainsi la voie à certaines possibilités de saisie/confiscation par les autorités judiciaires.

En matière de collaboration avec le SPF Finances, nous rappellerons que la CTIF dispose de diverses possibilités pour obtenir des informations de ce dernier. En 2023, elle a ainsi reçu de nombreuses informations qui lui ont été communiquées en vertu de l'article 79, § 2, 2° de la loi du 18 septembre 2017 mais a également très régulièrement fait usage de la possibilité qui lui est offerte par l'article 81, § 1, 4° de cette même loi de requérir des renseignements utiles à l'accomplissement de sa mission auprès du SPF Finances.

L'échange d'informations comprend le partage de listes de sociétés soupçonnées d'être un maillon d'une fraude organisée à la TVA en tant que '*missing traders'*. Le fait que ces sociétés étaient souvent connues de la CTIF dans le cadre d'un réseau de blanchiment d'argent confirme le lien entre la criminalité organisée et les fraudes fiscales graves et démontre l'importance de la coopération entre la CTIF et le SPF Finances.

Le nombre de dossiers transmis en raison d'indices sérieux de blanchiment de capitaux provenant notamment de la fraude fiscale grave étant à nouveau très important, cette collaboration s'est également traduite par l'envoi par la CTIF d'un nombre croissant d'informations pertinentes issues de

ces transmissions au ministre des Finances, et ce en application de l'article 83, § 2, 5° de la loi du 18 septembre 2017. Ce type de communications peut notamment avoir un important effet préventif. A titre d'exemple, la mise en avant précoce de nombreux acteurs défaillants permet entre autres la radiation de leur numéro TVA.

1.1.3. La corruption

Constatations relatives aux dossiers transmis

Au cours de l'année écoulée, la CTIF a transmis dix nouveaux dossiers aux autorités judiciaires identifiant la corruption, le détournement par des personnes exerçant une fonction publique ou la fraude au détriment des intérêts financiers de l'Union européenne comme principales criminalités sous-jacentes au blanchiment de capitaux.

Si ce nombre est inférieur à celui de 2022, où une grande partie des dossiers pouvait être liée à des enquêtes très médiatisées sur la corruption et le détournement de fonds publics à grande échelle, il est resté à un niveau similaire à celui de la période 2019-2021.

Les déclarations de soupçon à l'origine de ces dix dossiers provenaient principalement, comme les autres années, d'établissements de crédit, même si des informations particulièrement utiles ont également été fournies à la CTIF par des homologues étrangers, sous la forme de demandes de renseignements ou de communications spontanées d'informations.

La CTIF a analysé en profondeur les informations reçues et les a enrichies d'informations auxquelles elle a directement accès, d'informations et de renseignements obtenus par l'intermédiaire des entités assujetties et d'autres partenaires (notamment les services de renseignement, l'Office de lutte antifraude de la Commission européenne (OLAF) et les CRF étrangères), ainsi que de renseignements provenant de sources externes librement accessibles.

De l'analyse réalisée par la CTIF, il ressort que les dossiers concernaient, entre autres, des fonctionnaires belges, une personne ayant une fonction publique dans une institution de l'Union européenne et des personnes associées à des personnalités politiquement exposées en Afrique centrale ou du Nord.

Les transactions suspectes dans les dossiers étaient plutôt simples et consistaient principalement en des transferts nationaux, des opérations en espèces (dépôts ou retraits de comptes bancaires belges) et en des transferts internationaux. Ces dernières transactions comprenaient des transferts à partir de comptes détenus en nom propre par les intervenants dans des centres financiers internationaux en Europe ou en Asie.

La CTIF a lié les ***transactions suspectes*** au blanchiment de capitaux résultant de diverses formes de corruption et de détournement de fonds, notamment dans les cas suivants :

- un paiement national sur le compte d'un belge exerçant une fonction publique a été suspecté de représenter la réception d'un pot-de-vin dans le cadre d'une transaction immobilière ;
- les transferts (internationaux) sur les comptes belges de deux autres agents publics étaient plus que probablement liés au blanchiment de capitaux provenant d'un détournement de fonds par un agent public ou d'une corruption publique passive (corruption en tant que facilitateur du crime organisé) ;
- dans d'autres cas, les transactions étaient associées au blanchiment de capitaux provenant de la corruption dans le secteur médical ou à la corruption dans le cadre d'une transaction commerciale avec un Etat étranger et/ou au détournement par un PEP[9] d'une juridiction placée sous la surveillance renforcée du GAFI ;
- un transfert international depuis le compte d'un membre de la famille par alliance d'un chef d'Etat étranger en faveur de son compte en Belgique faisait sans doute partie d'un système mis en place pour blanchir des avoirs détournés d'un fonds souverain étranger. D'autres flux financiers transfrontaliers ont ensuite été liés au blanchiment de capitaux provenant d'un régime de RBI (régime de résidence des investisseurs) étranger géré par un intermédiaire commercial dans une juridiction offshore ;
- enfin, certaines transactions ont également mis en évidence d'éventuelles fraudes avec des fonds de l'Union européenne.

[9] Personne politiquement exposée.

Dans certains cas, les fonds illégalement acquis ont été utilisés pour l'achat de biens immobiliers de grande valeur ou pour effectuer des travaux d'embellissement au domicile des intéressés ou encore ont été transférés sur les comptes (d'épargne) des intéressés dans leur pays d'origine ou en Belgique.

Communication d'informations aux CRF étrangères impliquant des PEP

En 2023, la CTIF a de nouveau notifié à plusieurs CRF étrangères des transactions suspectes impliquant des PEP de leurs pays. Ces communications ont été effectuées en application de l'article 53.1 de la quatrième directive anti-blanchiment[10] et dans le cadre du traitement des déclarations reçues en lien avec les services de 'banque correspondante'.

Contexte plus large

Conformément à l'article 41 de la loi du 18 septembre 2017, les entités assujetties sont tenues de prendre des mesures de vigilance renforcées lorsqu'elles effectuent des transactions occasionnelles ou établissent des relations d'affaires avec des PEP, des membres de la famille de ces personnes ou des personnes connues pour être étroitement associés à ces personnes. En novembre 2023, la Commission européenne a publié une liste de fonctions publiques importantes qui pourraient faciliter l'identification du PEP dans l'Union européenne[11].

Cette liste comprend les fonctions publiques importantes au niveau des 27 États membres de l'Union européenne[12], au niveau des organisations internationales accréditées sur le territoire des Etats membres et au niveau des institutions et organes de l'Union européenne.

Dans son rapport annuel 2022, la CTIF a souligné l'impact négatif de la corruption sur l'état de droit. En 2023, la CTIF a de nouveau transmis au parquet quelques dossiers dans lesquels la corruption aurait pu servir de catalyseur à la criminalité organisée ou cibler une éventuelle ingérence étrangère et une influence dans les processus démocratiques. L'effet néfaste et déstabilisant de la corruption et de l'ingérence a également été soulevé au cours de l'année écoulée par les partenaires externes de la CTIF.

Bien que la CTIF ne soit pas directement impliquée dans les enquêtes sur les investissements étrangers en Belgique, elle est consciente des risques liés à l'opacité des financements étrangers, non seulement en matière de blanchiment de capitaux, mais aussi de financement du terrorisme. Dans ce contexte, la CTIF a suivi les discussions menées au sein du '*Radicalisation Awareness Network*'[13] dans le cadre d'un projet visant à mieux comprendre et combattre la menace des financements étrangers non désirés au sein de l'Union européenne.
L'année 2024 sera une année électorale dans plus de 60 pays à travers le monde. Il est bien connu que le financement des campagnes et des partis politiques peut être utilisé par des acteurs privés et des États étrangers pour influencer et interférer dans les élections. D'autre part, les conflits internationaux conduisent de plus en plus de gouvernements à ajuster leurs stratégies nationales en matière de marchés et de dépenses publiques. Cela peut entraîner un risque accru de corruption.

1.1.4. L'escroquerie

Tendances observées

Depuis de nombreuses années, l'escroquerie est la principale infraction sous-jacente au blanchiment dans les dossiers transmis par la CTIF aux autorités judiciaires. C'est à nouveau le cas en 2023. Avec 341 dossiers transmis, il s'agit du même ordre de grandeur qu'en 2022.

Certains de ces dossiers concernent des ***mules financières***, à savoir des personnes physiques qui, sciemment ou non, ont permis que leur compte bancaire et/ou leur carte bancaire et leur code PIN soient utilisés par des criminels pour blanchir de l'argent obtenu par toutes sortes d'escroqueries. Il

[10] Conformément à l'article 53, paragraphe 1, de la quatrième directive anti-blanchiment, la CTIF, lorsqu'elle reçoit une déclaration d'opérations suspectes se rapportant à un autre Etat membre, transmet toutes les informations pertinentes contenues dans la déclaration à la CRF de cet Etat membre. La présence d'un PEP est l'un des critères de pertinence qui devrait conduire à un transfert rapide des informations vers la CRF européenne dans le pays d'origine du PEP.
[11] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:C_202300724&qid=1709304577565
[12] Pour rappel: la liste des fonctions exactes identifiées comme des fonctions publiques importantes en Belgique figure également à l'annexe IV de la loi du 18 septembre 2017.
[13] Le *Radicalisation Awareness Network* est un réseau de personnes (y compris des autorités locales, des services répressifs, des experts et des universitaires) qui, sous la direction de la Commission européenne, échangent leurs expériences sur la manière d'aborder les questions (politiques) de la radicalisation et de l'extrémisme violent en Europe

s'agissait ici principalement d'escroqueries en ligne pour lesquelles des méthodes sophistiquées ont été utilisées pour tromper les victimes.

Au cours de l'année 2023, la CTIF a participé à un projet, mené conjointement par le Groupe Egmont, le GAFI et Interpol, sur les flux financiers illicites résultant de la cyberfraude (*Cyber-Enabled Fraud*, dénommée ci-dessous CEF). Le projet s'est concentré sur la fraude liée ou réalisée par des technologies de l'information et de la communication, impliquant la criminalité transnationale[14], et des techniques d'ingénierie sociale[15].

Bien que cette fraude puisse prendre diverses formes, l'analyse s'est concentrée sur la fraude par courriel d'entreprise (*Business Email Compromis* ou BEC)[16], la fraude par hameçonnage ou phishing[17], la fraude par usurpation d'identité via les médias sociaux et les télécommunications[18], la fraude à l'investissement en ligne[19], la fraude romantique en ligne[20] et la fraude à l'emploi[21] (ci-après désignées collectivement par le sigle CEF).

Le rapport[22] montre que la CEF est une criminalité organisée transfrontalière en pleine expansion et que le blanchiment de capitaux provenant de la CEF est facilité par des réseaux professionnels de blanchiment, qui font partie intégrante du groupe criminel en charge de la CEF ou qui, en tant qu'organisations distinctes, fournissent des services de blanchiment selon le modèle du '*crime as a service*', et par des prestataires de services professionnels impliqués dans le processus de blanchiment d'argent de la CEF.

Le blanchiment est généralement réalisé très rapidement après la fraude, par le biais d'un réseau de comptes détenus par des personnes physiques (mules financières) ou des personnes morales (sociétés fictives ou légitimes) auprès d'institutions financières de différents types (banques, établissements de paiement, fournisseurs de services d'actifs virtuels). D'autres techniques de blanchiment de capitaux peuvent également être utilisées, telles que l'utilisation des espèces, le blanchiment basé sur le commerce et les services (TBML/SBML[23]) et des techniques qui renforcent l'anonymat des actifs virtuels.

Les conclusions du rapport en matière d'escroqueries rencontrent celles de la CTIF.

Les dossiers transmis par la CTIF révèlent notamment comment les victimes européennes de la CEF ont effectué des paiements en faveur de comptes existants ou nouvellement ouverts, détenus par des mules financières auprès de banques ou d'établissements de paiement en Belgique. Les mules financières transféraient ensuite assez rapidement ces fonds vers des comptes belges ou étrangers à leur nom ou au nom de tiers auprès de banques traditionnelles, de banques en ligne, d'établissements de paiement ou d'établissements de monnaie électronique, vers des services de transfert d'argent en ligne ou des plateformes de crypto actifs.

---

[14] Tels que les acteurs transfrontaliers ou les flux financiers.
[15] Techniques dans lesquelles les victimes sont manipulées pour divulguer des renseignements confidentiels ou personnels.
[16] Fraude où les victimes reçoivent des instructions par courrier électronique prétendument de la part de clients ou de fournisseurs et dans lesquelles elles sont invitées à transférer de l'argent vers de nouveaux comptes de paiement.
[17] Fraude qui incite les victimes à divulguer des informations sensibles telles que des données personnelles, des renseignements bancaires ou des identifiants de connexion à des comptes. Les criminels utilisent ensuite les informations pour détourner l'argent des victimes de leurs comptes de paiements, ouvrir de nouveaux comptes bancaires ou effectuer des opérations frauduleuses
[18] La fraude à l'identité via les médias sociaux et dans les télécommunications comprend des scénarios où les victimes sont contactées par l'entremise d'application mobile ou de médias sociaux (WhatsApp, Facebook, Instagram, LinkedIn, X,...) par des criminels prétendant être des fonctionnaires du gouvernement, des membres de la famille ou des amis qui profitent des émotions des victimes pour leur soutirer de l'argent, pour prendre le contrôle des comptes de paiement ou pour effectuer des activités financières telles que demander des prêts ou ouvrir des comptes pour recevoir des produits du crime
[19] Fraude où les victimes sont induites en erreur par de fausses annonces ou des conseillers en ligne sur des plateformes inexistantes ou fausses (frauduleuses) pour investir ou échanger des actifs virtuels ou fiduciaires.
[20] Fraude où les victimes sont amenées à transférer de l'argent aux criminels après avoir été convaincues de s'engager dans une relation amoureuse.
[21] Fraude dans laquelle de fausses offres d'emploi sont publiées sur les plateformes de médias sociaux et les victimes sont convaincues d'effectuer des dépôts pour obtenir l'emploi ou d'acheter des produits pour augmenter les ventes sur une plateforme d'échanges.
[22] GAFI – Interpol – Groupe Egmont (2023), Flux financiers illicites de fraude cybernétique, GAFI, Paris, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html
[23] Service Based Money Laundering.

D'autres dossiers présentent clairement comment les produits de la fraude à l'investissement en ligne dont avaient été victimes des particuliers étrangers, ont été blanchis par le biais des comptes bancaires de sociétés écrans belges, souvent des entreprises du secteur de la construction, par des réseaux professionnels de blanchiment. Les transactions effectuées sur les comptes de ces sociétés écrans révèlent l'utilisation de techniques de blanchiment telles que la compensation et le TBML par l'intermédiaire de sociétés nationales et étrangères actives dans divers secteurs, notamment l'alimentation et le textile.

La CTIF a également transmis des dossiers pour blanchiment de capitaux résultant d'une *fraude au crédit*. Il s'agissait de fraudes portant sur des prêts octroyés par des établissements de crédit ou de paiement en Belgique sur la base de faux documents d'identité, de fausses fiches salariales ou d'autres documents falsifiés. Les montants empruntés ont souvent été transférés sur les comptes bancaires de mules financières, puis partiellement retirés en espèces ou transférés vers d'autres personnes physiques en Belgique ou à l'étranger en vue d'être utilisés pour des paiements par carte bancaire.

La majorité des types de fraude répertoriés incluent un élément d'usurpation d'identité. L'identité de la CTIF a également été utilisée dans des tentatives de fraudes (en ligne).

Enfin, la CTIF a également transmis aux autorités judiciaires des dossiers relatifs à des fraudes de type plus conventionnel, telles que les escroqueries liées à la vente de services à domicile dans lesquelles des démarcheurs font du porte-à-porte pour proposer des travaux d'entretien (démoussage de toitures, asphaltage des allées, etc.) en vue de facturer un prix nettement plus élevé que le prix convenu pour des travaux mal ou non effectués. Ces escroqueries pourraient dans certains cas être liées aux activités de groupes criminels organisés étrangers, qui ont blanchi le produit de la fraude par l'utilisation abusive du commerce international.

Déclarations de soupçon d'escroqueries et de fraudes

En 2023, la CTIF a reçu des informations sur d'éventuelles escroqueries et fraudes principalement dans les cas suivants :

- des établissements de crédit, établissements de paiement et établissements de monnaie électronique ont signalé, dans de nombreux cas, l'utilisation de comptes de passage par des mules financières ;
- des bureaux de change ont signalé des transferts d'argent effectués directement par des victimes ou par des mules financières ;
- la FSMA a échangé des informations avec la CTIF principalement au sujet de plateformes frauduleuses de trading en ligne[24] et d'offres de crédit frauduleuses[25]. Il s'agissait principalement de numéros de comptes bancaires étrangers ou d'adresses de portemonnaies électroniques vers lesquels des victimes belges avaient transféré de l'argent ou étaient invitées à le faire. Elle a également fourni des informations sur des comptes bancaires et des portefeuilles crypto utilisés dans la fraude de type *recovery room*[26] ;
- le SPF Economie a communiqué à la CTIF des informations sur les numéros de comptes belges ou étrangers utilisés pour des escroqueries ;
- les CRF étrangères ont informé la CTIF au sujet des numéros de comptes belges sur lesquels les victimes étrangères d'escroqueries avaient transféré de l'argent ou lui ont demandé d'analyser les opérations effectuées par l'intermédiaire de ces comptes ou de suspendre leur utilisation.

[24] Via de fausses plateformes en ligne d'apparence très professionnelle, les escrocs piègent les consommateurs en leur promettant des investissements incroyablement lucratifs dans les cryptos, les produits Forex, les CFD, les matières premières ou les métaux précieux. Les victimes potentielles sont généralement attirées par de fausses publicités sur les réseaux sociaux ou des plateformes vidéo en ligne.

[25] Dans cette forme de fraude, le consommateur, qui se trouve souvent déjà dans une situation financière précaire, entre en contact via Internet avec des prêteurs sans licence qui lui offrent un prêt à des conditions favorables. Sous prétexte de l'octroi du prêt, le consommateur est invité à payer toutes sortes de frais fictifs tels que les frais administratifs, les frais d'assurance, etc. Finalement, le consommateur ne reçoit pas le prêt demandé et ne peut pas récupérer les sommes versées.

[26] Dans ce type de fraude, les victimes d'une précédente fraude à l'investissement sont contactées par une entité qui leur promet de récupérer les fonds perdus. Pour récupérer l'argent, l'entité demande aux victimes de payer une avance. Cette somme n'est qu'un prétexte pour extorquer à nouveau de l'argent aux victimes. En fin de compte, les victimes ne récupèrent ni leur argent perdu, ni les avances supplémentaires.

Lors du traitement de ces dossiers, la CTIF cherche constamment l'équilibre entre, d'une part, le déploiement des ressources et, d'autre part, une contribution active à la lutte contre les différentes formes de fraudes selon une approche fondée sur le risque. Celle-ci repose sur le principe d'une utilisation maximale des compétences spécifiques des différents partenaires impliqués dans la lutte contre la fraude, en diffusant, dans la mesure du possible, les informations disponibles, et ce dans les limites légales.

Cette approche repose sur une combinaison de la transmission d'informations aux autorités judiciaires au sujet des principales mules financières ou de réseaux et d'un partage d'informations avec les homologues étrangers de la Cellule afin de les avertir des fraudeurs ou des mules financières qui opèrent dans leur pays, en vue de faciliter l'analyse des « comptes ou portefeuilles collectifs» et de mettre fin à certains flux financiers, ou, mieux encore, de permettre le recouvrement de fonds à l'étranger.

L'information qui n'est pas externalisée n'est pas considérée comme perdue, mais constitue une source essentielle d'informations pour l'analyse stratégique et le traitement des nouvelles déclarations et informations reçues par la CTIF.

Perspective

La fraude en ligne devrait encore augmenter à l'avenir, les fraudeurs en ligne et les cybercriminels continueront d'exploiter les nouvelles technologies pour maximiser les revenus tirés de la fraude. Europol affirme que se prémunir contre la fraude induite par l'IA (par exemple, la fraude impliquant le clonage de voix ou la génération de fausses images et vidéos) deviendra une nécessité absolue en matière de lutte contre la fraude en ligne[27]. L'Office européen de police prévoit également, qu'avec l'utilisation croissante des technologies innovantes, l'écosystème du crime en tant que service est susceptible de continuer à se développer et d'avoir un effet multiplicateur sur la criminalité organisée.

La prévention, la vigilance et la prudence restent essentielles pour prévenir des escroqueries. La coopération et l'échange d'informations en temps utile avec les partenaires (inter)nationaux restent également cruciaux dans la lutte contre le blanchiment de capitaux résultant d'escroqueries.

La CTIF a poursuivi ses efforts dans ce domaine en 2023. Au niveau national, la CTIF a travaillé avec le secteur financier, entre autres, à l'élaboration d'un formulaire de déclaration qui permet une déclaration et un traitement plus efficaces des déclarations en matière de fraude.

La CTIF a également participé à des échanges au niveau stratégique avec plusieurs autorités nationales compétentes dans le cadre de la Plateforme nationale de lutte contre la fraude de masse.

Au niveau international, la CTIF s'est opposée à plusieurs reprises à l'exécution d'opérations sur des comptes bancaires nationaux à la demande d'une CRF et a partagé de nombreuses informations dans le cadre de fraudes éventuelles avec des homologues étrangers.

1.2. Évolutions des techniques

1.2.1. Les prestataires de services de blanchiment

Afin de passer sous les radars des mécanismes croissants de surveillance du système financier légal, les organisations criminelles sont amenées à sous-traiter le blanchiment de leurs capitaux à des spécialistes. Ces derniers ne sont généralement ni des membres des groupes responsables des infractions sous-jacentes, ni des participants à celles-ci. Ils interviennent comme prestataires de services en vue de donner une apparence de licéité à des flux financiers d'origine illicite, issus d'activités criminelles multiples et diverses.

Les facilitateurs de blanchiment

La professionnalisation du blanchiment engendre un risque accru de voir les titulaires de professions financières et non financières être instrumentalisés par les criminels dans le cadre de leurs missions afin d'être utilisés en tant que facilitateurs de blanchiment.

[27] Voir, entre autres, Europol (2023), Systèmes de fraude en ligne: une toile de tromperie, Europol Spotlight Report Series, Office des publications de l'Union européenne, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Plusieurs dossiers transmis en 2023 confirment la réalité de ce risque et illustrent, en outre, l'implication de professionnels du droit et du chiffre en tant que facilitateurs aux spécialités diverses et complémentaires. Les dossiers révèlent comment ces professionnels offrent leurs ***services et conseils*** à des criminels. L'assistance fournie revêt diverses natures : accompagnement à la création de sociétés, élaboration du plan financier, constitution de sociétés, acquittement des frais de constitution, inscription auprès de la Banque carrefour des entreprises et de l'Administration de la TVA, préparation de bilans, fiches de salaires et fiches TVA, fourniture d'un siège social, de locaux, d'une adresse commerciale, administrative ou postale.
Il découle de l'ensemble des éléments que les professionnels concernés ont mis leurs compétences au service de divers réseaux criminels. Ils sont intervenus en tant que facilitateurs dans la mise en œuvre de mécanismes frauduleux tendant à indiquer qu'ils sont, à tout le moins, conscients des activités illicites menées au sein des sociétés auxquelles ils offrent leurs services.

A plusieurs reprises lors de l'exercice écoulé, la CTIF a avisé les autorités de contrôle concernées, en vue de l'application d'éventuelles sanctions, lorsque des entités relevant du contrôle de ces autorités étaient impliquées en tant qu'intervenants dans des dossiers transmis par la CTIF.

Les blanchisseurs professionnels

Un nombre croissant de dossiers illustre l'implication d'individus qui, en échange d'une commission sur leur service de blanchiment, usent de leur expertise et de leur infrastructure pour donner aux activités des criminels une apparence de légitimité, tout en permettant à ces derniers de rester dans l'ombre.

Pour ce faire, les schémas de blanchiment mis en place par les blanchisseurs professionnels reposent sur une constellation de sociétés et de comptes bancaires, et disposent d'un très grand nombre d'hommes de paille et de mules, tant en Belgique qu'à l'étranger, permettant, à chaque étape, d'opacifier les chaînes de blanchiment.

Les blanchisseurs professionnels offrent un ***service 'à la carte'*** en fonction des besoins des criminels. Ceux-ci peuvent leur confier l'ensemble du processus de blanchiment ou certaines parties et choisir la forme sous laquelle ils souhaitent recevoir leurs capitaux : argent liquide, produits de luxe, biens d'investissement ou biens immobiliers. Pour ce faire, les fonds sont d'abord collectés, éventuellement transportés et injectés dans le système financier. Les fonds circulent ensuite entre les comptes de sociétés écrans à travers les frontières, en utilisant des techniques telles que la compensation et le TBML pour dissimuler davantage l'origine illicite, avant d'être investis.

Cette tendance, présente de manière croissante dans les dossiers transmis par la CTIF, est également observée au niveau international.

Les sociétés en tant que vecteurs de blanchiment polycriminel

Les dossiers transmis sont caractérisés par le ***rôle central joué par des sociétés écrans*** constituées en série et intervenant comme vecteur de blanchiment. Certains secteurs, réputés sensibles en matière de fraude et de blanchiment, sont plus particulièrement utilisés, tels que la construction, le nettoyage industriel, l'horeca, le transport, l'import-export ou le commerce de voitures. Plusieurs dossiers, révélant notamment des liens avec la criminalité organisée, illustrent particulièrement le rôle joué par des sociétés agissant en tant que vecteurs de blanchiment polycriminel. Les montants en jeu se comptent souvent en millions d'EUR par dossier sur une période de quelques mois.

Différentes initiatives ont été menées par ou avec la CTIF, telles que la sensibilisation des parquets au sujet des sociétés écrans agissant comme vecteurs de blanchiment polycriminel ou les contacts récurrents de la CTIF avec la Cellule Prévention du blanchiment du SPF Economie.

1.2.2. Les paiements pour compte de tiers

Mécanisme

Les réseaux professionnels de blanchiment impliqués dans une grande partie du blanchiment provenant du trafic de stupéfiants et de diverses autres infractions sous-jacentes utilisent pour ce faire un certain nombre de techniques spécifiques. Les plus connues sont la compensation et le TBML, en plus du recours à des facilitateurs de blanchiment et des sociétés écrans comme évoqué ci-dessus. Cependant, au cours des dernières années, une technique est ressortie de l'analyse de nombreuses transactions dans les dossiers, à savoir les paiements pour compte de tiers ou, en anglais, '*third party payments (TPPs)*'.

Les *TPPs* sont des 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 d'un bien ou d'un service payé par un tiers qui n'est ni acheteur ni vendeur. Dans le cadre de circuits de paiements légaux, plusieurs fournisseurs de *TPPs* sont apparus sur le marché au cours des dix dernières années. Ils veillent à ce que les obligations de paiement soient respectées au sein de plateformes de services et fournissent une forme de '*settlement*' entre les fournisseurs et les clients sur ces plateformes. De cette façon, ils se chargent du suivi des paiements pour les vendeurs et offrent souvent une forme de garantie aux acheteurs, à savoir que le paiement n'est effectif que lorsqu'il est livré selon les conditions. Un exemple de ces services sont les plateformes de location de vacances, où les propriétaires de biens sont payés non pas par les locataires mais par la plateforme, qui, en plus de l'arrangement pratique, contrôle également les flux financiers.

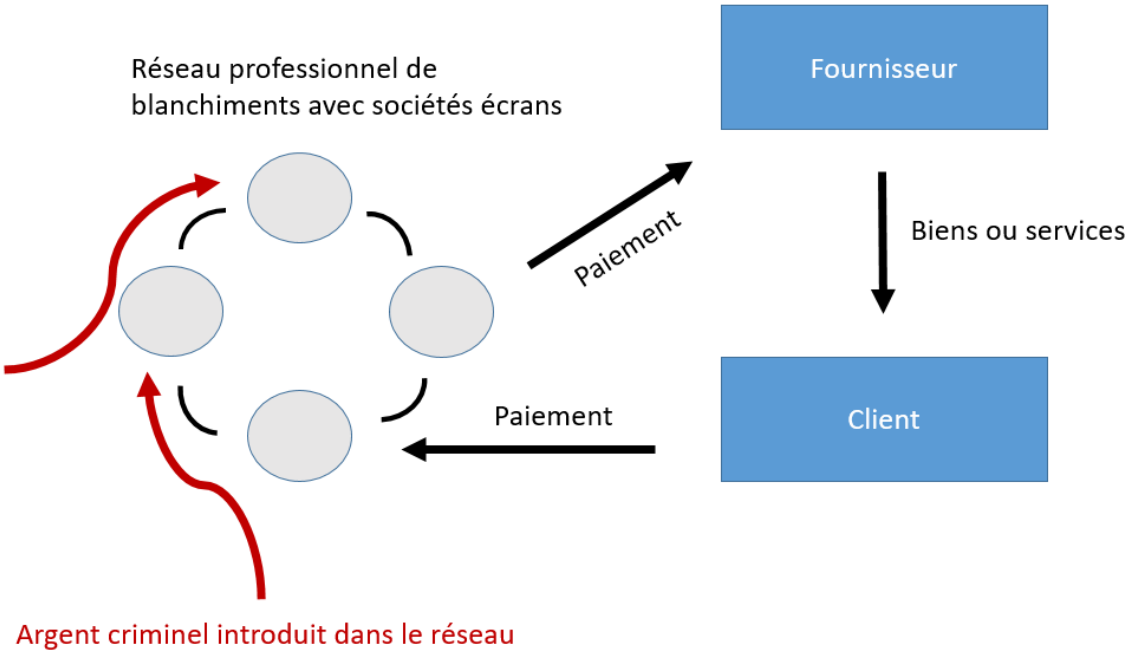
Dans le secteur des paiements, de nombreux prestataires de services de paiement sont actifs et, contre rémunération, surveillent et prennent en charge les obligations de paiement des clients. La digitalisation du secteur des paiements et l'augmentation des services en ligne ont entraîné une très forte croissance des paiements par des tiers.

Utilisation abusive par les réseaux professionnels de blanchiment

À l'instar de l'économie licite, où certains processus opérationnels tels que la comptabilité ou la maintenance de l'infrastructure informatique sont sous-traités à des prestataires de services spécialisés, une évolution généralisée vers une plus grande spécialisation est également observée dans le monde criminel. Si le développement des réseaux professionnels de blanchiment en est une bonne illustration, il apparaît également que, dans le cadre des paiements pour compte de tiers, une technique du système financier légal peut facilement être adoptée dans le monde criminel.

Ainsi, dans un contexte de blanchiment, les paiements par des tiers sont utilisés pour dissimuler les liens financiers et compliquer le suivi des flux d'argent. Lorsque des sociétés, situées dans certaines régions hors de l'Union européenne et considérées comme présentant un risque financier, souhaitent acheter des biens ou des services auprès de sociétés européennes, elles peuvent être confrontées à des coûts élevés ou à des obstacles administratifs lors du paiement. Le système bancaire formel est alors souvent évité, et un réseau informel est recherché afin de pouvoir effectuer le paiement. Le fournisseur, qui reçoit le paiement d'un tiers - une société ayant accès au système bancaire européen - est payé correctement en référence à la facture, et le client évite des coûts administratifs élevés ou de lourdes procédures de contrôles. Dans certains pays, il existe des réseaux financiers informels qui combinent ce service avec des services de transferts de fonds (hawala).

Bien que ce service ne soit généralement pas réglementé au niveau juridique, cela ne rend pas l'origine de l'argent illégale. Néanmoins, les organisations criminelles actives dans le domaine du blanchiment se sont inspirées du système de paiement par des tiers pour en faire une utilisation abusive, profitant du fait que les sociétés n'ont plus aucun soupçon quant à la réception de paiements provenant d'autres parties que les acheteurs. Ainsi, en échange d'une faible commission, des réseaux professionnels de blanchiment offrent des services de paiement dans des domaines où le système financier régulier fonctionne parfaitement en parvenant à mélanger des fonds issus d'activités criminelles avec des paiements cadrant dans le commerce légitime (voir schéma).



Dans les réseaux professionnels de blanchiment, que la CTIF considère depuis plusieurs années comme le principal vecteur de blanchiment en Belgique, les paiements entre des sociétés écrans et des sociétés licites sont très fréquents. Souvent, ces flux financiers entre des sociétés dont les activités n'ont aucun lien entre elles n'ont pas de justification économique. Les comptes des sociétés écrans traitent des millions d'euros de paiements en quelques mois, un flux financier qui ne peut être expliqué par l'activité réelle ou la taille de l'entreprise. Au débit, des transferts sont effectués vers d'autres sociétés écrans, mais aussi, dans la dernière phase du processus, vers des sociétés qui exercent une activité officielle. Il s'agit parfois même de grandes entreprises réputées dans des secteurs tels que l'alimentation, la chimie ou les produits pharmaceutiques.

Outre les réseaux professionnels de blanchiment, les organisations criminelles elles-mêmes ont également recours à des paiements pour compte de tiers pour rémunérer leurs membres en nature. Des montres, des voitures de luxe, mais aussi des cuisines ou des billets de football sont livrés et facturés à des personnes qui ont rendu un service à l'organisation, mais qui sont payées par des sociétés contrôlées par l'organisation criminelle. La facture est ensuite falsifiée au niveau de la comptabilité. Les fournisseurs sont payés correctement - même si ce n'est pas par le client - et ne remettent pas en question la transaction. Les facilitateurs ainsi rémunérés pour les services rendus ne doivent pas justifier des fonds entrants sur leurs comptes, évitant ainsi la détection par les institutions financières.

Paiements pour compte de tiers dans le cadre du contournement des sanctions

Enfin, l'utilisation de paiements pour compte de tiers se produit également dans le cadre de la fourniture de services de 'banque correspondante' (COBA), c'est-à-dire de services liés aux paiements et au commerce internationaux. Le règlement des transactions financières par l'intermédiaire de SWIFT[28] implique un réseau de banques ayant des relations réciproques et pouvant agir en tant qu'agents pour d'autres institutions financières, généralement à l'étranger. Les banques intermédiaires surveillent et filtrent également ces transactions pour les personnes et les opérations à destination et en provenance de pays sanctionnés ou à haut risque.

Cependant, la technique du TPP peut être utilisée à mauvais escient pour permettre indirectement à des pays ou à des individus sanctionnés d'accéder au système financier international.

Par exemple, il apparaît que dans les centres financiers ou les pays situés à proximité immédiate des pays sanctionnés, des sociétés écrans sont créées ou des bureaux de change, clandestins ou non, sont utilisés pour permettre les paiements entre le pays ou les entités sanctionnés et des sociétés en

[28] Society for Worldwide Interbank Financial Telecommunication, organisation coopérative internationale pour la transmission de messages financiers fondée en 1973.

Europe par le biais de paiements pour compte de tiers. En outre, la technique du TPP est également utilisée dans les pays sanctionnés eux-mêmes.

La Belgique compte quelques banques actives dans le domaine de la 'banque correspondante' et disposant d'un réseau étendu. La CTIF a mené des analyses sur les TPPs et le contournement des sanctions sur la base d'informations fournies par ces banques. Les transactions COBA constituent une source d'information cruciale pour mieux comprendre cette typologie.

L'analyse des informations COBA oriente donc fortement vers des réseaux utilisés pour contourner les sanctions contre le pays, mais aussi éventuellement pour effectuer des achats dans des contextes de prolifération. Une autre partie des informations COBA s'inscrit dans d'importantes transactions financières potentiellement liées à des faits de corruption dans différents pays étrangers.

L'analyse des TPPs dans le cadre du COBA permet à la CTIF d'inscrire les investigations belges dans un contexte international et de mieux appréhender les risques de blanchiment, de financement du terrorisme et de prolifération.

Toutefois, vu la nature même des informations COBA (souvent exclusivement internationale sans lien direct avec des entités belges), la CTIF externalise la plupart de celles-ci sous forme d'échanges spontanés vers les CRF homologues concernées par les activités suspectes détectées.

***