



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Bureau de communication en matière de blanchiment d'argent (MROS)

Rapport annuel 2024



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Bureau de communication en matière de blanchiment d'argent (MROS)

Rapport annuel 2024

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol
Bureau de communication en matière de blanchiment d'argent (MROS)
3003 Berne

Tél. : (+41) 58 463 40 40
E-mail : meldestelle-geldwaescherei@fedpol.admin.ch

Internet : <https://www.fedpol.admin.ch>

Table des matières

1	Avant-propos	6
2	Développements stratégiques importants	8
2.1	Orientation et objectifs du MROS pour la période de 2024 à 2027	8
2.2	Évaluation nationale des risques – Rapport sectoriel sur le risque de financement de la prolifération	8
2.3	Partenariat public-privé (PPP) – Swiss FIPPP	9
2.4	Cellule de renseignement financier (CRF) 2.0	10
2.5	Projets et événements du MROS	11
2.5.1	Financial Intelligence against Human Trafficking (FIAHT)	11
2.5.2	Rapport des typologies	12
2.5.3	Crypto Symposium 2.0 du MROS	13
2.5.4	Chinese Underground Round Table	13
3	Statistique annuelle du MROS	14
3.1	Constatations générales 2024	14
3.2	Communications de soupçons	15
3.3	Communications de soupçons par secteur d'activité des IF	15
3.4	Bases légales des communications	17
3.5	Infractions préalables	18
3.6	Éléments à l'origine des soupçons	18
3.7	Dénonciations aux autorités de poursuite pénale	19
3.8	Retour d'information des autorités pénales	19
3.9	Financement du terrorisme	21
3.10	Criminalité organisée	22
3.11	Communications de soupçons en rapport avec les monnaies virtuelles	22
3.12	Remise d'informations au sens de l'art. 11a LBA	23
3.13	Communications de rupture de la relation d'affaires au sens de l'art. 9b LBA	24
3.14	Échange d'informations avec les homologues étrangers (CRF)	24
3.15	Échange d'informations avec les autorités suisses	25
4	Tendances	26
4.1	Jeux d'argent en ligne	26
4.2	Pédopornographie et actifs virtuels	29
4.3	Interdiction du Hamas	30
5	Pratique du MROS	32
5.1	Immédiateté vs degré de clarification des communications – Position du MROS	32
5.2	Interprétation de l'art. 11a LBA – Justification des demandes de renseignements	33
5.3	Obligation de communiquer et droit de communiquer	34
5.4	Définition des « autorités de poursuite pénale »	35
6	Coopération internationale dans la lutte contre le blanchiment d'argent	36
6.1	Groupe Egmont	36
6.2	GAFI	36
6.2.1	Généralités	36
6.2.2	Évaluations mutuelles	37
6.3	Taskforces	38
6.4	Rencontres bilatérales	38
7	Organisation du MROS	39

1 Avant-propos

Des chiffres records ont encore été atteints en 2024 dans pratiquement toutes les catégories faisant l'objet du présent rapport. Le MROS¹ a enregistré au total 27 901 entrées dans son système d'information goAML², ce qui représente une hausse de près de 30% par rapport à l'année précédente. Depuis l'introduction de goAML en 2020, le volume des données entrantes a plus que triplé. Le MROS reçoit en moyenne 107 rapports par jour ouvrable: communications de soupçons (STR³ et SAR⁴), réponses des intermédiaires financiers (IF) à ses demandes⁵, annonces de rupture de relations d'affaires⁶, informations spontanées, demandes et réponses d'autorités tant nationales qu'internationales, à savoir de cellules de renseignement étrangères (CRF), ainsi que les notifications des décisions et jugements d'autorités pénales⁷.

En 2024, le MROS a reçu au total 15 141 communications de soupçons, ce qui correspond à une augmentation de 27,5 % par rapport à 2023 (11 876). Ainsi, 59 communications en moyenne ont été enregistrées par jour ouvrable. Les communications de soupçons représentaient environ 55% des rapports entrants. Ce taux n'a cessé de diminuer ces dernières années: il y a dix ans, il était encore supérieur à 90%. Cette évolution s'explique par la forte hausse des activités d'assistance administrative entre le MROS et les autorités nationales, mais également avec ses homologues étrangers. Elle montre clairement que les autorités travaillent aujourd'hui plus souvent en réseau et procèdent à des clarifications auprès de services externes. Ce constat vaut aussi notamment pour le MROS. Le renseignement financier repose sur l'échange actif d'informations et l'interaction avec les différentes parties prenantes. Afin de traiter efficacement d'importants volumes de données, il faut des rapports structurés et d'une qualité suffisante tant sur le plan de la forme que du contenu. Le MROS a continué de constater divers niveaux de qualité dans les communications de soupçons. La raison serait la pression sur les coûts – mais il y a de toute évidence

également conflit entre le principe d'immédiateté des communications de soupçons et le degré de clarification (cf. ch. 5.1).

Le MROS a transmis au total 1043 dénonciations aux autorités de poursuite pénale en 2024, leur nombre ayant donc augmenté de plus de 20% par rapport à l'année précédente. Il a à chaque fois mis à la disposition des autorités de poursuite pénale un rapport d'analyse comprenant les informations pertinentes. Celles-ci peuvent être issues de différentes communications de soupçons qui n'ont pas forcément été transmises au MROS la même année et contenir des éléments provenant de diverses autorités suisses ou étrangères. Au cours de l'exercice sous revue, le MROS a transmis aux autorités de poursuite pénale 1,9 communication de soupçons en moyenne par dénonciation. Ce nombre moyen a augmenté au cours des dernières années (1,3 en 2021; 1,4 en 2022; 1,8 en 2023). Environ une transmission aux autorités de poursuite pénale sur cinq contenait en outre des informations en réponse à une ou à plusieurs demandes adressées par le MROS à des IF ou à des intermédiaires tiers en vertu de l'art. 11a LBA⁸. En 2024, le MROS a aussi davantage eu recours à l'instrument qu'est l'information spontanée (art. 29 LBA): il a transmis au total 358 informations spontanées aux autorités suisses, ce qui constitue une hausse de 79% par rapport à l'année précédente. Il diffuse ses informations de manière opportune et implique rapidement les autorités destinataires en vue de la transmission.

Le nombre de dénonciations déposées auprès des autorités de poursuite pénale n'est qu'un indicateur partiel de l'efficacité et de l'efficience de l'activité d'analyse. D'une part, il faut tenir compte de la performance globale, c'est-à-dire des analyses effectuées qui contribuent à la transmission des dénonciations et des informations spontanées. D'autre part, le processus appliqué est également crucial, car il détermine la quantité d'informations

¹ Money Laundering Reporting Office Switzerland

² government office Anti-Money Laundering

³ Suspicious transaction reports

⁴ Suspicious activity reports

⁵ Le MROS émet des demandes au sens de l'art. 11a de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA; RS 955.0).

⁶ Au sens de l'art. 9b LBA

⁷ Au sens de l'art. 29a LBA

⁸ Loi du 10 octobre 1997 sur le blanchiment d'argent (LBA; RS 955.0).

effectivement traitées dans le cadre d'une analyse. Le MROS a amélioré ces deux indicateurs au cours de 2024.

Il a reformulé, pour la période de 2024 à 2027, ses objectifs stratégiques et son profil concernant les tâches principales dont il doit s'acquitter en vertu de la loi, affinant ainsi les trois domaines « Renseignement », « Coopération » et « Prévention » (cf. ch. 2.1). Ses réflexions ont également porté sur les défis futurs auxquels les CRF seront confrontées et sur les capacités et les instruments dont le MROS aura besoin à l'avenir pour les relever. Ces défis seront identifiés dans le cadre d'une étude qui devrait être achevée en 2025 (cf. ch. 2.4).

Le 7 novembre 2024, le Swiss Financial Intelligence Public Private Partnership (Swiss FIPPP), composé de douze établissements financiers et du MROS, a officiellement lancé ses activités. La place financière suisse dispose ainsi d'un partenariat public-privé et se met au niveau des autres centres financiers internationaux (cf. ch. 2.3). À la fin octobre 2024, le MROS a organisé la deuxième édition du Crypto Symposium. Cet événement s'adressait au secteur financier spécialisé dans le domaine des crypto-actifs et des actifs virtuels (AV). Les retours ont été très positifs. Dans ce segment financier encore récent, les échanges entre les autorités et le secteur revêtent une importance capitale, c'est pourquoi le MROS organisera un événement similaire en 2025 (cf. ch. 2.5.3). Dans le présent rapport annuel, la rubrique « Typologies » a été supprimée et il est renvoyé à la place à un rapport des typologies sur la page Internet du MROS (cf. ch. 2.5.2), ce qui permet à ce dernier de fournir au secteur financier des études de cas actuelles tout au long de l'année.

2 Développements stratégiques importants

2.1 Orientation et objectifs du MROS pour la période de 2024 à 2027

Le MROS est le bureau central auquel sont communiqués en Suisse les cas de soupçons liés au blanchiment d'argent et au financement du terrorisme; il remplit les tâches d'une CRF. Son mandat, qui est inscrit dans la loi et l'ordonnance correspondantes, comprend les trois tâches principales suivantes :

- **Renseignement** : le MROS reçoit les communications de soupçons que lui envoient les IF et les négociants en vertu de la LBA et du code pénal⁹. Il procède à ses propres analyses et enrichit les communications de soupçons reçues d'informations supplémentaires. Il décide ensuite au cas par cas de la transmission ou non d'une dénonciation aux autorités de poursuite pénale.
- **Coopération** : le MROS mène des échanges avec d'autres autorités nationales et des CRF étrangères sur les questions opérationnelles et stratégiques par la voie de l'assistance administrative.
- **Prévention** : le MROS contribue à évaluer les risques nationaux de blanchiment d'argent et de financement du terrorisme. Il effectue des analyses stratégiques et partage les résultats obtenus avec des autorités, le secteur financier et le grand public.

Ces trois tâches principales ne doivent pas être considérées séparément, car elles forment un tout indissociable. Le renseignement en est cependant le fondement : c'est sur lui que la coopération et la prévention reposent.

Pour la période de 2024 à 2027, le MROS a reformulé les objectifs stratégiques découlant de son mandat légal¹⁰. Ces objectifs illustrent comment le MROS remplit ce mandat, quelles sont ses priorités et comment il utilise sa marge de manœuvre. Périodiquement redéfinis, ils répondent aux évolutions

de la lutte contre le blanchiment d'argent et la criminalité ainsi qu'aux défis qui en résultent, faisant le lien entre le mandat légal et l'activité concrète du MROS.

La nouvelle stratégie du MROS définit six objectifs et treize mesures. Elle fixe des priorités claires en matière de grande criminalité et offre, grâce aux analyses prévues, une valeur ajoutée dans la lutte contre la criminalité à ses partenaires directs – à savoir les autorités suisses, les CRF étrangères et le secteur financier. Le nombre de rapports en constante augmentation au fil des ans et le manque de ressources contraignent le MROS à agir en fonction des risques¹¹. Outre la concentration systématique sur certains types d'infractions, le MROS mise dans sa stratégie sur la rationalisation des processus de communication et de traitement. Le développement de l'infrastructure informatique constitue une priorité supplémentaire. Des outils d'analyse modernes sont essentiels pour traiter efficacement des données de masse et produire des analyses pertinentes. Il importe également de coopérer de manière active et ad hoc avec les différentes parties prenantes : secteur privé et financier, autorités suisses et homologues étrangers. Dans un environnement mondialisé, la criminalité financière ne peut être combattue qu'en joignant les forces. Il est primordial de réunir les diverses parties autour de la même table afin d'examiner ensemble les problématiques qui se posent.

2.2 Évaluation nationale des risques – Rapport sectoriel sur le risque de financement de la prolifération

L'appréciation des risques liés au blanchiment d'argent et au financement du terrorisme est un élément important de la stratégie de lutte contre la criminalité en Suisse. Notre pays a déjà publié deux évaluations nationales des risques générales (*national risk assessment*, NRA; 2015¹² et 2021¹³). Le Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le finan-

⁹ Code pénal suisse, RS 311.0

¹⁰ Cf. [Stratégie du MROS 2024-2027](#).

¹¹ Cf. explications concernant l'approche fondée sur les risques dans le [Rapport annuel 2023 du MROS](#), ch. 2.2.

¹² [Première évaluation nationale des risques \(NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), juin 2015

¹³ [Deuxième évaluation nationale des risques \(NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), octobre 2021

cement du terrorisme (GCBF) en est le mandant et assume la responsabilité de leur élaboration. En tant que membre du GCBF et responsable du sous-groupe « Analyse des risques », le MROS est chargé de rédiger des rapports sur les risques. Le GCBF publie périodiquement des NRA sur des thématiques liées aux risques et les met à jour en permanence.

Outre ces appréciations générales, le GCBF publie régulièrement des évaluations sectorielles des risques. Le 17 septembre 2024, il a adopté le rapport sectoriel *National Risk Assessment: Proliferationsfinanzierung* (NRA sur le risque de financement de la prolifération; uniquement en allemand), élaboré par le MROS en collaboration avec le Secrétariat d'État à l'économie¹⁴.

La prolifération des armes de destruction massive et de leurs vecteurs constitue une menace pour la paix et la sécurité internationale. La prévention du financement de la prolifération repose sur un cadre juridique international et national complexe. Tout en mettant l'accent sur l'Iran et la Corée du Nord, le rapport sectoriel dresse un tableau des risques mondiaux en la matière et expose ceux qui sont spécifiques à ces deux pays.

S'agissant de la Suisse, il dresse notamment les constats suivants:

- C'est dans le négoce de matières premières, le commerce de cryptomonnaies et les opérations de banque correspondante que les risques de financement de la prolifération sont jugés les plus importants. Il existe également un risque global découlant des manœuvres de contournement adoptées par des sociétés écrans.

- L'Iran présente des risques liés au négoce car, contrairement à la Corée du Nord, le pays n'est pas exclu de la chaîne de valeur. Ce dernier pays, en revanche, pose un risque plus élevé dans le domaine de la cybercriminalité et dans l'utilisation connexe de cryptomonnaies.

Le rapport recommande de renforcer le dispositif visant à combattre le financement de la prolifération en élargissant le mandat du GCBF à cette lutte et en créant un groupe de travail interdépartemental dédié à ce thème. Par ailleurs, il convient d'améliorer la base de données et de mieux sensibiliser davantage le secteur privé.

2.3 Partenariat public-privé (PPP) – Swiss FIPPP

L'échange d'informations entre les autorités et le secteur privé rend la lutte contre le blanchiment d'argent plus efficace. Ces deux acteurs doivent donc collaborer de manière ad hoc et être en mesure d'échanger des informations sur les menaces, les risques, les méthodes et les tendances dans les domaines du blanchiment d'argent et du financement du terrorisme. Au cours des dix dernières années, divers PPP ont été mis en place au niveau international à des fins d'échange d'informations financières.

Cette évolution a également incité la Suisse à lancer son propre PPP dans le domaine du blanchiment d'argent et du financement du terrorisme. Le 7 novembre 2024, le Swiss FIPPP a lancé son activité lors d'une séance plénière constitutive¹⁵. Des travaux préparatoires qui ont duré près de deux ans ont précédé son lancement officiel. Il s'agissait d'ana-



Fig. 1 : Logo du Swiss FIPPP.

¹⁴ Communiqué de presse du Conseil fédéral du 9 décembre 2024, [Rapport sur le risque de financement de la prolifération \(uniquement en allemand\)](#)

¹⁵ [Swiss Financial Intelligence Public Private Partnership \(Swiss FIPPP\)](#), consulté le 31 janvier 2025

lyser dans quel cadre une coopération public-privé était possible en Suisse¹⁶. L'échange d'informations dans le domaine stratégique, qui est au cœur du partenariat entre le MROS et les acteurs suisses des marchés financiers, vise à identifier les risques et les menaces et à renforcer de manière conjointe et durable le dispositif de lutte. Une coopération à vocation tactique, dans le cadre de laquelle des informations sur des cas et des personnes spécifiques seraient échangées, n'est pas prévue à ce jour et nécessiterait des modifications légales. Le Swiss FIPPP réunit le MROS et douze institutions financières initiatrices : Banque Julius Bär & Cie SA, Banque Vontobel SA, Banque Lombard Odier & Cie SA, Bitcoin Suisse SA, Deutsche Bank (Suisse) SA, HSBC Private Bank (Suisse) SA, Raiffeisen Suisse société coopérative, Société Générale Corporate & Investment Banking, UBS SA, Banque Valiant SA, Banque cantonale de Zurich et Zurich compagnie d'Assurances SA. Il n'est pas exclu que le cercle des membres évolue.

Une séance plénière est prévue au moins deux fois par an. En outre, des groupes de travail consacrés à des thèmes spécifiques se réunissent régulièrement. Les activités du Swiss FIPPP sont coordonnées par un comité dont les membres sont élus par l'assemblée plénière. L'organisation et la communication sont assurées par le MROS. Le Swiss FIPPP informera de ses activités et des résultats obtenus aussi bien dans un rapport annuel que de manière ad hoc et en fonction des destinataires.

2.4 Cellule de renseignement financier (CRF) 2.0

Lors de sa création en 1998, le MROS employait quatre personnes et recevait 173 communications de soupçons. Vingt-six ans plus tard, il compte près de 55 collaborateurs et le nombre de communications de soupçons s'est démultiplié pour atteindre 15 000 transmissions. Dans son rapport annuel 2023, il a expliqué les raisons réglementaires et opérationnelles de cette forte hausse du volume de communications¹⁷. Mais que signifient ces évolutions pour les CRF sur le plan organisationnel ? De quoi les CRF ont-elles besoin pour pouvoir conti-

nuer à remplir leur mandat légal et les tâches qui en découlent ?

Le blanchiment d'argent, qui est le principal moteur de la criminalité organisée, a considérablement gagné en complexité ces dernières années. Les réseaux internationaux, l'évolution des techniques pour blanchir des fonds et l'utilisation de nouvelles technologies (par ex. AV) rendent la lutte contre le blanchiment d'argent et le financement du terrorisme toujours plus ardue et complexe. Alors que par le passé, l'activité du MROS se cantonnait principalement à la réception et à la transmission de communications de soupçons, c'est sur le renseignement que l'accent est clairement mis ces dernières années. Sont aujourd'hui au premier plan la mise en réseau des informations et la création de valeur ajoutée pour les autorités de poursuite pénale en aval, grâce à des analyses concises et à l'interaction avec les autorités nationales, les homologues étrangers et le secteur financier. Ces activités sont nécessaires pour combattre efficacement le blanchiment d'argent et le financement du terrorisme. Cependant, il est impératif de développer les CRF dans les domaines centraux que sont l'infrastructure informatique et le personnel, afin de suivre les évolutions de la politique mondiale, de s'acquitter des tâches croissantes et de répondre aux exigences grandissantes.

Infrastructure informatique

Pour accomplir leur travail, les CRF ont besoin de logiciels répondant à leurs exigences et aux évolutions mondiales dans le respect du cadre légal (notamment les dispositions relatives à la protection des données). La capacité à collecter et à analyser de grandes quantités de données provenant de diverses sources, y compris le renseignement de sources ouvertes (*open source intelligence*, OSINT), ne cesse de gagner en importance. Les CRF doivent être en mesure d'interpréter les informations issues de transactions financières, de banques de données et d'OSINT. L'intelligence artificielle et l'apprentissage automatique jouent ici un rôle déterminant aux fins de détection et d'identification précoces des activités suspectes. Les nouvelles technologies permettent aux CRF d'accroître

¹⁶ Rapport du MROS: [Partenariat public-privé \(PPP\) relatif à l'échange d'informations dans la lutte contre le blanchiment d'argent et le financement du terrorisme](#), mars 2023

¹⁷ Cf. [Rapport annuel 2023 du MROS](#), ch. 2.1.

leur efficacité et d'approfondir leur compréhension des menaces émanant du blanchiment d'argent et du financement du terrorisme.

Planification du personnel

La complexité des faits à analyser, les questions juridiques et l'utilisation d'outils spécifiques exigent une planification stratégique du personnel au sein des CRF. Il est primordial pour ces dernières de recruter des spécialistes et de fidéliser les collaborateurs qualifiés. Les CRF doivent offrir des conditions de travail attrayantes et disposer des liquidités nécessaires pour attirer et retenir ces talents à long terme. Elles ont besoin d'une certaine marge de manœuvre afin de planifier et d'utiliser les ressources de manière opportune.

Les progrès techniques fulgurants, qui offrent des moyens toujours plus nombreux et plus faciles d'accès pour le blanchiment d'argent et le financement du terrorisme, posent des défis de taille aux CRF dans le monde entier (et pas seulement en Suisse). En tant que partie intégrante de l'administration fédérale, le MROS doit composer avec un volume de communications et de données en constante augmentation, des ressources limitées, des contraintes budgétaires et le cadre juridique actuel. Cependant, il doit disposer des instruments idoines nécessaires afin de lutter contre la grande criminalité. Les limitations susmentionnées ne doivent pas être en totale contradiction avec la nécessité de ces instruments. Il est nécessaire de procéder à une valorisation qui vise l'efficacité d'une CRF.

Dans ce contexte, le MROS présentera en 2025 une étude sur le thème des « CRF 2.0 » visant à traiter les défis susmentionnés et à proposer des solutions. En fera également partie une analyse comparative, qui fournira des indications sur la position du MROS en comparaison internationale.

2.5 Projets et événements du MROS

En 2024, le MROS a lancé les projets et les événements ci-après. Il entendait ainsi mettre des instruments utiles à la disposition des autorités et du secteur privé et sensibiliser ces derniers en conséquence. Ces projets et ces événements ont permis d'établir des tendances et des indicateurs importants permettant de lutter de façon plus systématique contre le blanchiment d'argent et le financement du terrorisme.

2.0.1 Financial Intelligence against Human Trafficking (FIAHT)

La traite des êtres humains est l'une des branches les plus lucratives de la criminalité organisée. Il s'agit d'un crime transnational commis à l'abri des regards. L'Organisation internationale du travail estime que la traite des êtres humains génère chaque année dans le monde des bénéfices à hauteur de 236 milliards de dollars. C'est à chaque fois l'appât du gain qui prime, aux dépens des victimes exploitées. L'analyse approfondie des flux de paiement et des mouvements de compte, autrement dit la stratégie consistant à suivre l'argent (*follow the money*) appliquée par le MROS, contribue de manière essentielle à mettre au jour les activités illégales liées à la traite des êtres humains et à identifier les victimes.

Contexte

La législation suisse considère la traite des êtres humains comme une infraction préalable au blanchiment d'argent. Les IF sont par conséquent tenus de signaler au MROS tout soupçon de traite des êtres humains et d'infractions connexes. En Suisse, comme dans nombre d'autres pays européens, le nombre de communications de soupçons concernant la traite des êtres humains est extrêmement faible. Il existe un grand décalage entre l'ampleur de ce crime et le volume de communications transmises par les IF.



FIAHT Financial Intelligence against Human Trafficking

Fig. 2: Logo du projet FIAHT

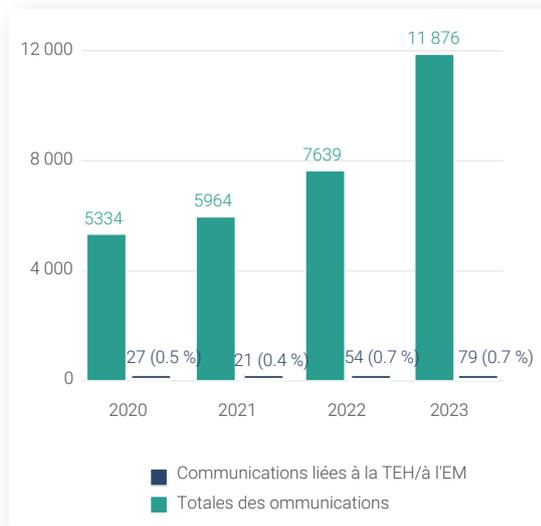


Fig. 3: Communications relatives à la traite des êtres humains par rapport au nombre total de communications de soupçons reçues par le MROS, 2020-2023.

Projet FIAHT

Avec le soutien du Bureau du représentant spécial et coordinateur pour la lutte contre la traite des êtres humains de l'Organisation pour la sécurité et la coopération en Europe, le MROS a lancé le projet Financial Intelligence Against Human Trafficking (FIAHT).

Ce projet avait pour objectifs :

- l'élaboration d'un guide de sensibilisation des IF ;
- le renforcement de la coopération et l'optimisation des processus opérationnels entre le MROS et les autres acteurs concernés grâce à la mise en place d'un partenariat multipartite.

Le MROS a pris la direction du projet lors de son lancement officiel, sous la forme d'une table ronde le 24 janvier 2024. En collaboration avec diverses autorités de poursuite pénale et de la Confédération, ainsi que des représentants du secteur financier et de la protection des victimes, des données et des informations ont été rassemblées dans le guide de sensibilisation FIAHT. Les jalons ont ainsi été posés afin d'intensifier les échanges entre les acteurs intéressés, une tâche également prioritaire. Le 25 novembre 2024, l'événement de clôture du

projet FIAHT a eu lieu à Berne et a été l'occasion de présenter le contenu du guide.

Guide FIAHT¹⁸

Ce guide propose des approches et des instruments clairs visant à aider les IF et les négociants à identifier les transactions et les comportements relevant de la grande criminalité, à savoir notamment :

- des **indicateurs** permettant de conclure à l'existence de traite d'êtres humains et d'infractions apparentées ;
- des **exemples pratiques** révélant comment les criminels dissimulent leurs gains et comment les IF peuvent détecter de tels agissements ;
- des **bonnes pratiques** montrant aux IF comment rédiger de manière efficace et précise une communication de soupçons afin de faciliter les analyses et les investigations en aval.

Dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent et la criminalité organisée, les mesures de sensibilisation sont déterminantes afin de réduire le décalage existant entre le nombre de communications de soupçons et les conséquences financières de ces crimes.

2.0.2 Rapport des typologies

Le mandat de prévention du MROS comprend la sensibilisation des IF et des négociants à la problématique du blanchiment d'argent, aux infractions préalables au blanchiment d'argent, à la criminalité organisée et au financement du terrorisme. Outre les publications régulières telles que les rapports annuels et les NRA, le MROS diffuse également des newsletters et élabore des lignes directrices spécifiques (par ex. *Alerts and typologies in the context of the terrorist attacks by Hamas and Palestinian Islamic Jihad (PIJ) on Israel on October 7, 2023* ou Guide FIAHT ; cf. ch. 2.5.1). Ces documents permettent de guider les IF et de leur fournir des bonnes pratiques.

À titre d'instrument de sensibilisation supplémentaire, le MROS a également mis en place un rapport des typologies¹⁹. Les typologies du blanchiment d'argent permettent de classer et d'analyser de façon systématique les méthodes et les procédures typiquement utilisées par les criminels afin

¹⁸ Publications du MROS

¹⁹ Sera transféré ultérieurement dans une base de données.

d'injecter des fonds illégaux dans le circuit économique légal. Ces modes opératoires englobent une multitude de techniques permettant aux criminels de dissimuler l'origine des fonds et d'en empêcher la confiscation. Le rapport des typologies aide les IF à identifier des indicateurs potentiels. C'est grâce à des faits anonymisés et simplifiés que le MROS crée ces typologies. Celles-ci permettent d'analyser clairement des situations complexes, favorisent l'observation différenciée et offrent une structure efficace afin d'identifier les schémas récurrents.

En mai 2025, le MROS publiera les premières typologies sur sa page Internet²⁰. La liste de ces typologies sera régulièrement mise à jour. S'adressant principalement aux IF et aux négociants, elle ne sera dans un premier temps publiée qu'en anglais.

2.0.3 Crypto Symposium 2.0 du MROS

Comme en 2023, le MROS a organisé le Crypto Symposium à la fin octobre 2024. Alors que la première édition s'était concentrée sur les défis liés au suivi des cryptomonnaies et à la détection des infractions liées à ces dernières, l'accent a été mis en 2024 sur les dangers concrets posés par l'utilisation des cryptomonnaies et les risques de fraude qui en découlent. Quelque 270 participants issus du secteur public tout comme de celui des finances et du conseil ont participé à cet événement. Divers représentants d'autorités suisses et étrangères et du secteur privé ont présenté des exposés.

Différents domaines de criminalité dans lesquels les cryptomonnaies sont utilisées frauduleusement ont été examinés. Les thèmes traités allaient de la cybercriminalité à l'utilisation illégale de cryptomonnaies par des sociétés de sécurité privées, en passant par le contournement des sanctions, le recouvrement d'actifs, les jeux de hasard et la fraude. Outre la classification des AV en vue des évaluations mutuelles que le GAFI effectuera, plusieurs autorités ont partagé leurs expériences concernant la gestion de la criminalité numérique et ont abordé la lutte contre la fraude à l'investissement. Un autre thème considéré était l'utilisation frauduleuse de cryptomonnaies dans le but de financer

des guerres et des troupes de mercenaires. Il a été souligné que des appels aux dons aux fins de financement d'activités militaires étaient organisés sur des plates-formes comme Telegram, ce qui pose des difficultés supplémentaires aux autorités de poursuite pénale.

En résumé, il apparaît nécessaire de renforcer la coopération nationale et internationale et d'utiliser de manière opportune des instruments techniques afin de combattre la crypto-criminalité croissante²¹.

2.0.4 Chinese Underground Round Table

Appelé *hawala* au Moyen-Orient et en Afrique, *hundi* en Asie du Sud, *fei ch'ein* ou *daigou* en Chine, le principe du transfert de fonds clandestin n'est pas nouveau : il est aussi vieux que le commerce transfrontalier. Les réseaux clandestins fonctionnent à l'écart du système bancaire légal, sans autorisation ni surveillance de l'État. On n'y trouve donc pas l'ombre d'un justificatif ni d'un numéro de compte bancaire, sans parler des autres données. Les transactions sont rapides, avantageuses et anonymes. C'est précisément ce qui rend ces banques clandestines si intéressantes pour la dissimulation et le transfert de fonds criminels et le financement du terrorisme. Malgré ces obstacles, les autorités de poursuite pénale parviennent régulièrement à mettre au jour des réseaux et des flux financiers. L'échange d'enseignements tirés des enquêtes couronnées de succès, d'analyses et de bonnes pratiques dans ce domaine est donc très important. C'est à cette fin que le MROS a organisé la première table ronde à l'échelon suisse sur le système bancaire clandestin chinois. La rencontre était principalement destinée aux autorités de poursuite pénale et de lutte contre le blanchiment d'argent nationales et internationales, qui participent activement à la lutte contre la criminalité organisée. fedpol, Europol, des autorités de poursuite pénale et des CRF de plusieurs pays européens étaient représentées à la table ronde²².

²⁰ Informations complémentaires sous [Publications du MROS](#)

²¹ Communiqué de presse de fedpol du 29 octobre 2024: [Crypto Symposium 2.0 du MROS: ensemble contre l'utilisation frauduleuse de cryptomonnaies](#)

²² Communiqué de presse de fedpol du 31 octobre 2024: [Première table ronde sur la lutte contre les banques clandestines](#)

3 Statistique annuelle du MROS

Le MROS établit une statistique anonymisée afin d'exploiter les informations concernant le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée et le financement du terrorisme au cours de l'exercice sous revue²³. Cette statistique comprend notamment les communications de soupçons des IF, les demandes de renseignements d'autorités étrangères analogues ainsi que les procédures faisant suite aux communications (cf. art. 23, al. 1, OBCBA²⁴).

3.1 Constatations générales 2024

- Le nombre de **communications de soupçons** transmises a encore nettement augmenté en 2024: le MROS en a reçu **15 141**, soit environ 59 par jour ouvrable. Par rapport à 2023 (11 876), ce nombre représente une hausse de 27,5%. Depuis que goAML a été introduit en janvier 2020, le volume des communications a presque triplé.
- Les communications de soupçons proviennent pour **92,3%** d'IF du **secteur bancaire** (moyenne 2015-2024: 90,1%).
- En 2024, le MROS a transmis aux IF **1016 demandes d'informations au sens de l'art. 11a LBA**.
- Par rapport à 2023, le MROS a transmis **+20,4% de dénonciations aux autorités de poursuite pénale**²⁵. Le MROS transmet à chaque fois aux autorités de poursuite pénale un rapport d'analyse contenant les informations pertinentes. Celles-ci peuvent contenir des informations provenant de différentes communications de soupçons qui n'ont pas forcément été transmises au MROS la même année, ainsi que des informations provenant de différentes autorités suisses ou étrangères. En 2024, le MROS a transmis en moyenne 1,9 communication de soupçons par dénonciation aux autorités de poursuite pénale. Là aussi, une augmentation constante du nombre moyen de communications de soupçons transmises par dénonciation est constatée²⁶. Environ une transmission sur cinq (18,9%) contenait en outre des informations issues d'une ou de plusieurs demandes adressées par le MROS à des IF ou des intermédiaires tiers en vertu de l'art. 11a LBA.
- L'échange d'informations entre le MROS et les autorités suisses est en augmentation. Par rapport à 2023, les **informations spontanées transmises par le MROS** à d'autres **autorités suisses** ont augmenté de 79%. En revanche, les demandes d'informations (447, soit une baisse de 35,8% par rapport à l'année précédente) et les informations spontanées (106, soit un recul de 10,9%) adressées par d'autres autorités suisses au MROS ont diminué.
- **L'échange d'informations avec des CRF étrangères** est également en hausse constante. En 2024, le MROS a reçu 780 demandes émanant de 96 CRF étrangères et 751 informations spontanées provenant de 45 pays.

²³ Exercice: du 1^{er} janvier au 31 décembre de l'année concernée

²⁴ Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent (OBCBA; RS 955.23)

²⁵ 1043 en 2024 et 866 en 2023

²⁶ 1,4 en 2022 et 1,8 en 2023

3.2 Communications de soupçons

En 2024, le MROS a reçu 59 communications de soupçons en moyenne par jour ouvrable, ce qui équivaut à 15 141 communications au total transmises par des IF ou des négociants et représente une augmentation supplémentaire de 27,5% par rapport à l'année précédente. Ce nombre a presque triplé depuis que goAML a été introduit en 2020 (cf. Fig. 4)²⁷.

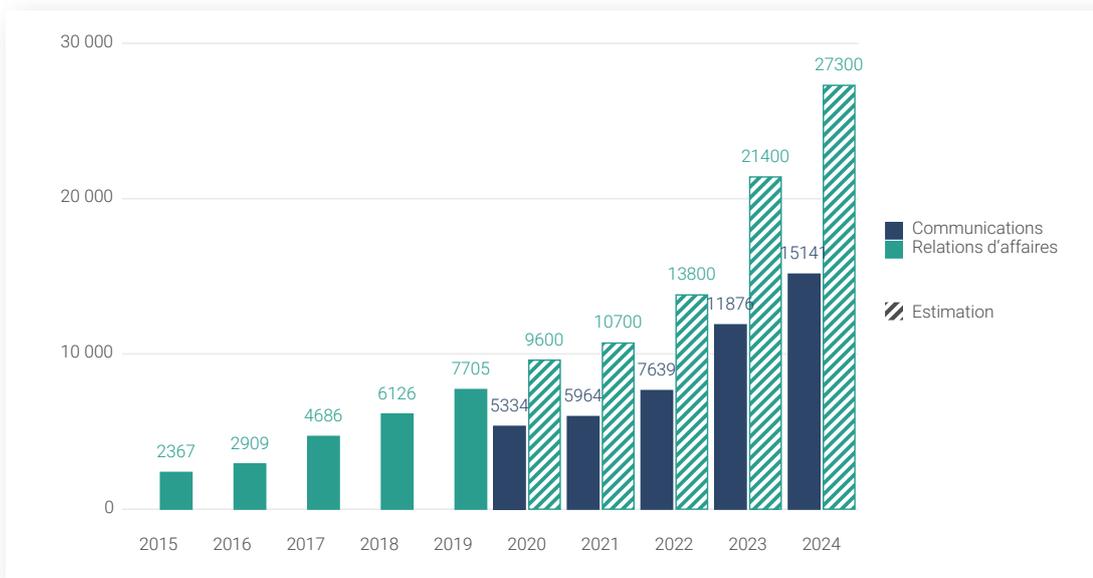
Comme le montre la Fig. 4, le nombre de relations d'affaires signalées chaque année a été multiplié par près de douze depuis 2015. Alors que cette année-là 2367 relations d'affaires suspectes avaient été communiquées au MROS, on en dénombrait environ 27 300 en 2024. Plusieurs raisons expliquent cette augmentation. D'une part, les IF sont de plus en plus sensibilisés à la problématique du blanchiment d'argent. D'autre part, les adaptations juridiques et les progrès de la numérisation (par ex. l'amélioration des outils de surveillance des transactions et d'analyse interne) jouent un rôle central²⁸.

3.3 Communications de soupçons par secteur d'activité des IF

Exactement 92,3% des communications de soupçons proviennent d'IF du secteur bancaire. Le comportement de ces IF influe de manière déterminante sur le nombre et le type de communications reçues par le MROS. La répartition des communications de soupçons entre les différents secteurs d'activité n'a guère changé depuis l'introduction de goAML (cf. tabl. 1).

Présentés depuis 2024 dans une catégorie distincte, les prestataires de services d'actifs virtuels (PSAV) et de fintech ont soumis 227 communications de soupçons au MROS (1,5%) au cours de l'exercice sous revue.

Fig. 4: Nombre de relations d'affaires signalées et de communications de soupçons 2015-2024



²⁷ La façon de compter les cas suspects a été adaptée avec l'introduction de goAML. Afin de permettre une comparaison avec les années précédentes, la fig. 4 présente le nombre moyen de relations d'affaires signalées par communication de soupçons transmise en 2019. Ce nombre s'élève à 1,8, ce qui signifie que les 15 141 communications de soupçons de 2024 correspondent à environ 27 300 relations d'affaires.

²⁸ Cf. explications dans le [Rapport annuel 2023 du MROS](#), ch. 2.1.

Tabl. 1 : Communications de soupçons par secteur, 2015-2024²⁹

Secteur	2015 ^A	2016	2017 ^A	2018 ^A	2019 ^A	2020 ^B	2021 ^B	2022 ^B	2023 ^B	2024 ^B	2024 en chiffres absolus	Moyenne 2015-2024
Banques	91,3%	86%	91%	88,8%	89,9%	89,5%	90,0%	91,6%	90,5%	92,3%	13973	90,1%
Prestataires de services de paiement	2,4%	4,4%	3,1%	4,4%	4,0%	3,5%	2,5%	2,0%	2,8%	2,2%	339	3,1%
Cartes de crédit	0,5%	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	1,6%	235	1,2%
PSAV / Fintech										1,5%	227	
Gérants de fortune / Conseillers en placement	1,9%	2,2%	1,9%	1,0%	0,9%	0,8%	1%	0,6%	0,8%	0,9%	137	1,2%
Maisons de jeu	0,1%	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	0,3%	47	0,5%
Opérations de crédit, de leasing, d'affacturage et de financement à forfait	0,3%	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	0,2%	37	0,3%
Maisons de titres	0,1%	0,1%	0,3%	0,1%	0,3%	0%	0,2%	0,1%	0,2%	0,2%	32	0,2%
Fiduciaires	2%	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	0,2%	30	0,8%
Autres intermédiaires financiers	0,2%	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2%	0,2%	24	1,3%
Négociants en matières premières et métaux précieux	0,3%	0,1%	0,2%	0%	0,3%	0,2%	0,5%	0,3%	0,3%	0,2%	23	0,2%
Assurances	0,5%	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	0,2%	23	0,7%
Bureaux de change	0%	0%	0%	0%	0%	0,1%	0,1%	0,3%	0,6%	0%	5	0,1%
Avocats et notaires	0,3%	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0%	0,1%	0%	5	0,1%
OAR	0%	0%	0%	0%	0,1%	0%	0%	0%	0,1%	0%	4	0%
Autorités (FINMA / CFMJ / GESPA)	0%	0%	0%	0%	0%	0%	0,1%	0%	0%	0%	0	0%
Négoce de devises	0%	0,1%	0%	0%	0,3%	0%	0%	0%	0%	0%	0	0%
Trustees	0%	0%	0%	0%	0%	0,1%	0,1%	0%	0%	0%	0	0%
Distributeurs de fonds de placement	0%	0%	0,1%	0%	0%	0%	0%	0%	0%	0%	0	0%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	15 141	100,0%

^A Selon l'ancienne manière de compter (par relations d'affaires)

^B Selon l'actuelle manière de compter (par communications)

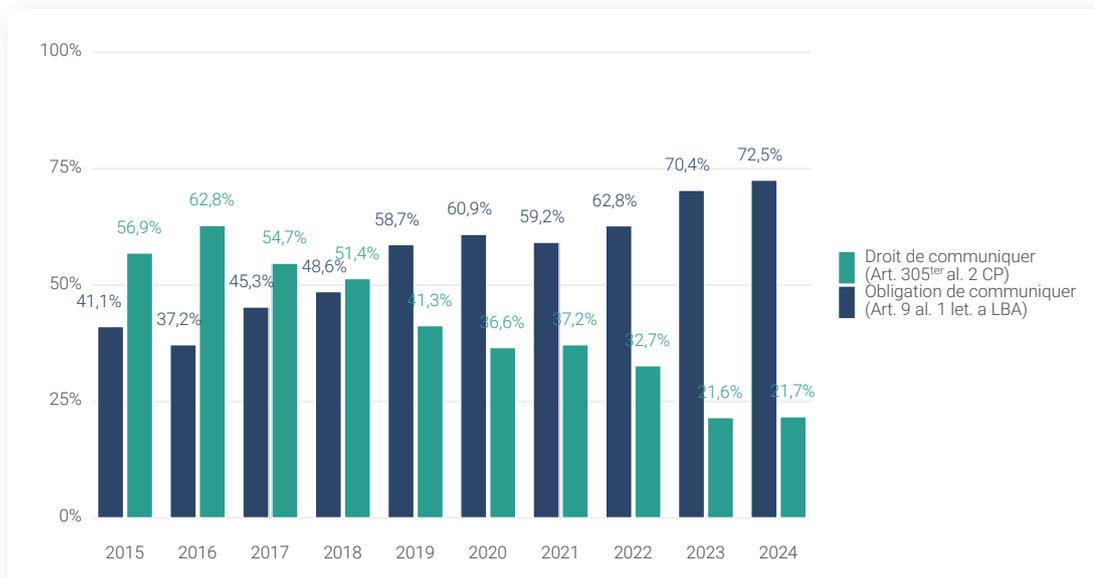
²⁹ Les chiffres absolus pour les années 2014 à 2023 sont présentés dans les rapports annuels du MROS des années correspondantes.

3.4 Bases légales des communications

La base légale d'une communication de soupçons dépend du degré de suspicion. S'ils ont des soupçons fondés, les IF ont l'obligation de les communiquer au MROS en vertu de l'art. 9, al. 1, let. a, LBA³⁰. S'ils n'ont que de simples soupçons, ils peuvent s'appuyer sur le droit de communiquer prévu à l'art. 305^{ter}, al. 2, CP³¹. En 2024, les communications transmises relevaient dans 72,5% des cas de l'obligation de communiquer (art. 9, al. 1, let. a, LBA; cf. Fig. 5) et dans 21,7% des cas du droit de communiquer (art. 305^{ter}, al. 2, CP). Dans 5,6% des cas, les IF ont en outre signalé qu'ils avaient rompu des négociations visant à établir une relation d'affaires en raison d'un soupçon fondé au sens de l'art. 9, al. 1, let. a, LBA (art. 9, al. 1, let. b, LBA; données non incluses dans la fig. 5)³².

Gagnant constamment en importance par rapport au droit de communiquer depuis 2018, l'obligation de communiquer a fait un bond en avant en 2023 (cf. rapport annuel 2023 du MROS, ch. 4.4). Après avoir enregistré une augmentation constante de l'obligation de communiquer ces dernières années, les statistiques montrent en 2024 pour la première fois une certaine consolidation du rapport existant entre l'obligation de communiquer et le droit de communiquer. Alors que le recours à l'obligation de communiquer dans le cadre d'une relation d'affaires existante a augmenté de 2,1% par rapport à l'année précédente, le droit de communiquer a enregistré une hausse marginale de 0,1%. Les communications des IF en cas d'interruption des négociations en vue d'établir une nouvelle relation d'affaires conformément à l'art. 9, al. 1, let. b, LBA ont reculé de 2,3%.

Fig. 5: Communications relatives à des relations d'affaires existantes par base légale 2015-2024



³⁰ « L'intermédiaire financier informe immédiatement le Bureau de communication en matière de blanchiment d'argent au sens de l'art. 23 (bureau de communication) s'il sait ou présume, sur la base de soupçons fondés, que les valeurs patrimoniales impliquées dans la relation d'affaires: 1. ont un rapport avec une des infractions mentionnées aux art. 260^{ter} ou 305^{bis} CP, 2. proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305^{bis}, ch. 1^{er}, CP, 3. sont soumises au pouvoir de disposition d'une organisation criminelle ou terroriste, 4. servent au financement du terrorisme (art. 260^{quinquies}, al. 1, CP) » (art. 9, al. 1, let. a, LBA).

³¹ « Les personnes visées à l'al. 1 ont le droit de communiquer au Bureau de communication en matière de blanchiment d'argent de l'Office fédéral de la police les indices fondant le soupçon que des valeurs patrimoniales proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305^{bis}, ch. 1^{er} » (art. 305^{ter}, al. 2, CP).

³² « L'intermédiaire financier informe immédiatement le Bureau de communication en matière de blanchiment d'argent [...] s'il rompt des négociations visant à établir une relation d'affaires en raison de soupçons fondés conformément à la let. a » (art. 9, al. 1, let. b, LBA).

3.5 Infractions préalables

Lors d'une communication, les IF indiquent à chaque fois l'infraction préalable ou les infractions préalables qu'ils présument. Ces dernières années, une dizaine d'infractions préalables différentes étaient le plus souvent mentionnées (cf. Fig. 6)³³. Les IF ont cité le plus fréquemment en 2024 l'escroquerie. Seule ou en combinaison avec d'autres infractions (cette part était de 57,2% de 2020 à 2023), celle-ci concernait 59,4% des communications. D'autres infractions préalables comme le faux dans les titres (7,1%; 12,1% de 2020 à 2023) ou l'abus de confiance (4,1%; 6,1% de 2020 à 2023) ont été beaucoup plus rarement nommées.

Les indications fournies par les IF sur les infractions préalables présumées constituent une première qualification importante reposant sur les clarifications qu'ils ont effectuées. La Fig. 6 ci-dessus présente les infractions que les IF présument lorsqu'ils soumettent une communication de soupçons. L'analyse faite par le MROS peut aussi

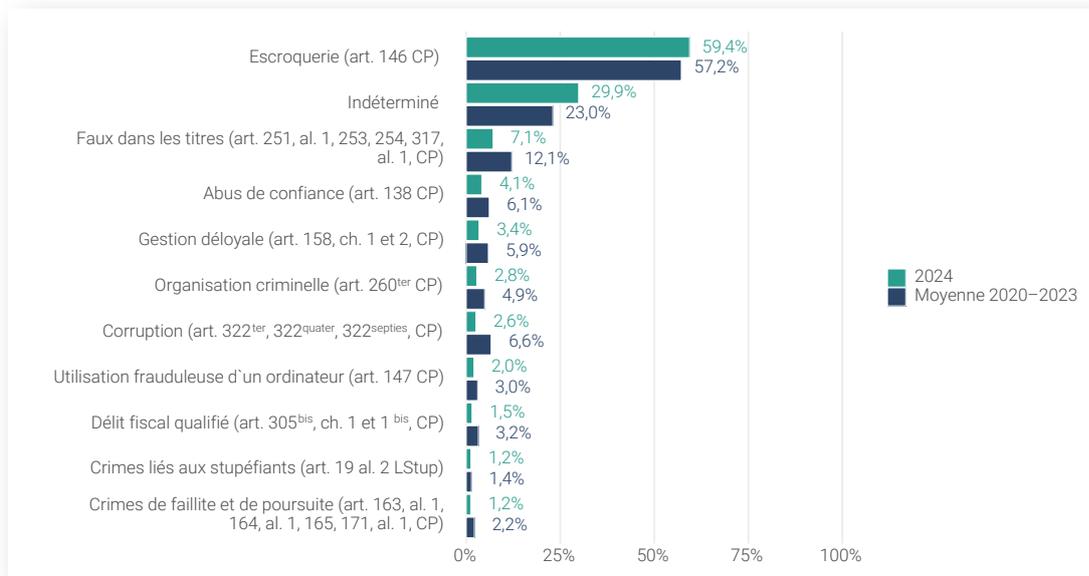
établir des soupçons laissant présumer une autre infraction³⁴.

En 2024, les IF indiquent ne pas être en mesure de mentionner une infraction préalable dans près d'une communication de soupçons sur trois (29,9%). Cette tendance n'a cessé de s'accroître au fil des ans et a continué de croître au cours de l'exercice sous revue. Le fait qu'environ un tiers des communications de soupçons soient soumises au MROS sans indication d'une infraction préalable a de vastes répercussions. Ce dernier doit alors mobiliser des ressources supplémentaires pour procéder à des clarifications permettant d'identifier l'infraction préalable.

3.6 Éléments à l'origine des soupçons

En principe, les IF soumettent une communication de soupçons au MROS après avoir surveillé des transactions (29,6% en 2024; 32% de 2020 à 2023; cf. Fig. 7)³⁵. Les autres éléments à l'origine

Fig. 6: Fréquence des infractions préalables présumées
2020-2024, Plusieurs réponses possibles



³³ Depuis l'introduction de goAML en 2020, plusieurs réponses peuvent être fournies. Il n'est ainsi pas possible d'effectuer une comparaison avec les statistiques antérieures à 2020.

³⁴ Une analyse plus détaillée des diverses infractions préalables au blanchiment d'argent a été effectuée en 2021 sous la direction du GCBF: [Deuxième évaluation nationale des risques \(NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), octobre 2021, pp. 25 à 29.

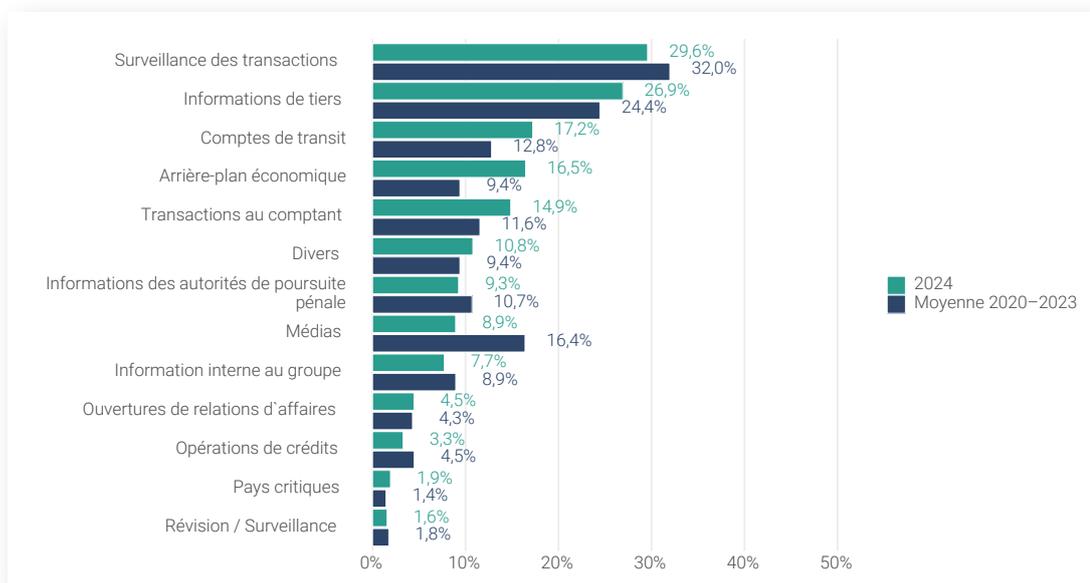
³⁵ Contrairement à ce qui prévalait avant 2020, le nouveau système d'information goAML permet aux IF de signaler plusieurs éléments qui les ont portés à concevoir des soupçons. Par contre, il n'est plus possible d'effectuer une comparaison précise de ces chiffres avec ceux des années antérieures à 2020.

des soupçons sont les informations provenant de tiers (sources d'information externes; 26,9%) et les comptes de transit (17,2%). Par rapport aux années précédentes, les IF ont indiqué bien plus souvent en 2024 que l'arrière-plan économique de la relation d'affaires n'était pas clair (16,5%; 9,4% de 2020 à 2023).

Le MROS a transmis 89,7% des dénonciations aux ministères publics cantonaux et 10,3% au Ministère public de la Confédération (MPC).

Comme les années précédentes, plus de la moitié des dénonciations ont été déposées auprès d'un nombre restreint de ministères publics cantonaux

Fig. 7: Principaux éléments à l'origine des soupçons
2020-2024, Plusieurs réponses possibles



3.7 Dénonciations aux autorités de poursuite pénale

En 2024, le MROS a transmis 1043 dénonciations aux autorités de poursuite pénale en vertu de l'art. 23, al. 4, LBA, ce qui représente une hausse de 20,4% par rapport à l'année précédente (866 en 2023). Ces dernières années, les dénonciations transmises par le MROS aux autorités de poursuite pénale s'appuient sur une base de plus en plus conséquente: alors qu'une dénonciation reposait en moyenne sur 1,4 communication de soupçons en 2022, ce nombre était de 1,9 en 2024.

Les 1043 dénonciations transmises contiennent des informations provenant de:

- 1481 communications reçues en 2024;
- 432 communications reçues en 2023;
- 32 communications reçues en 2022;
- 13 communications reçues en 2021;
- 5 communications reçues en 2020;
- 2 relations d'affaires signalées avant 2020.

– Zurich (17,9%), Vaud (12,4%) et Genève (10,2%) – ainsi qu'auprès du MPC (10,3%) (cf. tabl. 2).

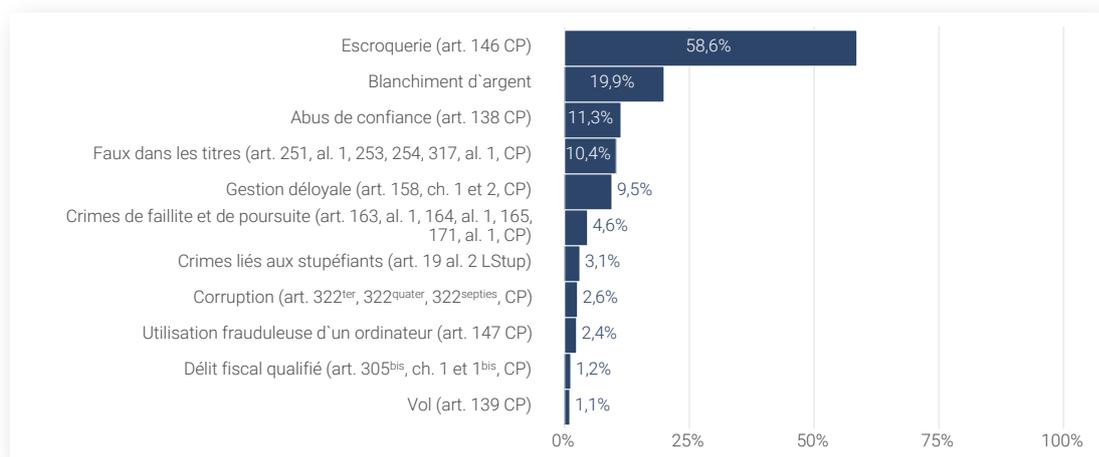
En 2024, sur l'ensemble des dénonciations aux autorités de poursuite pénale, le MROS a suspecté dans près de 60% des cas qu'une escroquerie pouvait être à l'origine des avoirs. Dans un cinquième des dénonciations, il a indiqué l'élément constitutif de l'infraction de blanchiment d'argent (cf. Fig. 8), par exemple lorsque le prévenu auteur de l'infraction préalable ne correspondait pas à la personne ayant blanchi les capitaux.

Tabl. 2: Dénonciations transmises par autorité de poursuite pénale 2020-2024

Autorité	2020	2021	2022	2023	2024	2024 en chiffres absolus	Moyenne 2020-2024
Zurich	18,9%	21,1%	20,4%	16,3%	17,9%	187	18,9%
Vaud	11,1%	11,6%	10,6%	8,3%	12,4%	129	10,8%
MPC	9,0%	9,1%	6,4%	13,0%	10,3%	107	9,6%
Genève	11,5%	11,3%	11,6%	17,6%	10,2%	106	12,4%
Berne	7,5%	6,7%	6,9%	6,5%	7,7%	80	7,1%
Argovie	5,3%	5,2%	6,7%	4,2%	5,7%	59	5,4%
Tessin	5,0%	4,8%	3,6%	4,6%	5,5%	57	4,7%
Saint-Gall	3,5%	4,0%	6,3%	5,3%	5,3%	55	4,9%
Lucerne	3,5%	2,9%	2,6%	2,5%	3,9%	41	3,1%
Bâle-Ville	2,6%	2,3%	2,3%	1,8%	3,2%	33	2,4%
Valais	2,7%	2,4%	3,0%	2,2%	2,9%	30	2,6%
Bâle-Campagne	2,1%	1,7%	2,3%	1,8%	2,2%	23	2,0%
Fribourg	2,7%	3,1%	2,1%	1,3%	2,1%	22	2,3%
Soleure	1,9%	2,0%	2,1%	1,4%	2,1%	22	1,9%
Thurgovie	3,0%	2,1%	2,6%	3,2%	1,7%	18	2,5%
Schwyz	1,0%	1,1%	1,9%	2,1%	1,5%	16	1,5%
Zoug	2,5%	2,6%	2,2%	2,2%	1,2%	12	2,1%
Grisons	1,5%	1,0%	1,1%	0,6%	1,1%	11	1,1%
Neuchâtel	2,3%	1,9%	1,7%	1,3%	1,0%	10	1,6%
Schaffhouse	0,5%	0,5%	0,6%	0,7%	0,6%	6	0,6%
Appenzell Rhodes-Extérieures	0,6%	0,8%	1,3%	0,9%	0,5%	5	0,8%
Jura	0,3%	1,0%	0,2%	0,7%	0,4%	4	0,5%
Appenzell Rhodes-Intérieures	0,0%	0,1%	0,2%	0,2%	0,3%	3	0,2%
Nidwald	0,3%	0,4%	0,6%	0,6%	0,3%	3	0,4%
Glaris	0,2%	0,1%	0,4%	0,6%	0,2%	2	0,3%
Obwald	0,2%	0,1%	0,2%	0,0%	0,2%	2	0,1%
Uri	0,3%	0,1%	0,2%	0,1%	0,0%	0	0,1%
Total	100,0%	100,0%	100,0%	100,0%	100%	1043	100,0%

Fig. 8: Fréquence des éléments constitutifs d'infraction dénoncés aux autorités de poursuite pénale, 2024

Plusieurs réponses possibles



3.8 Retour d'information des autorités pénales

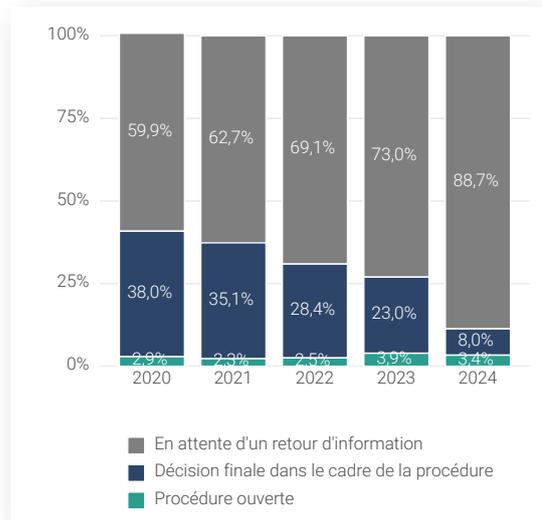
Conformément à l'art. 29a LBA, les autorités pénales annoncent sans délai au MROS toutes les procédures pendantes en rapport notamment avec le blanchiment d'argent, les organisations criminelles et terroristes et le financement du terrorisme³⁶. De plus, elles l'informent sans délai les décisions qu'elles ont prises sur les dénonciations qu'il leur a adressées³⁷. Ce retour d'information est essentiel à la mission du MROS, qui est d'apporter le meilleur soutien possible aux autorités de poursuite pénale.

Les statistiques du rapport annuel 2023 montrent que la plupart des dénonciations n'ont pas encore reçu de retour d'information, ce qui s'explique par le long temps de traitement par les autorités pénales³⁸. Si l'on considère uniquement les dénonciations transmises plus de douze mois avant la fin de 2024 (période allant de 2020 à 2023), il apparaît que, le 31 décembre 2024, aucune information concernant l'état d'avancement de la procédure n'est disponible pour près de deux tiers des cas transmis (64,3%). Ce constat est valable pour plus de la moitié des dénonciations déposées en 2020 pour lesquelles la procédure n'est toujours pas close.

En 2024, les autorités pénales ont annoncé au MROS 82 ordonnances pénales et 48 jugements rendus en lien avec des dénonciations qu'il avait déposées, ainsi que 262 ordonnances de non-entrée en matière ou décisions de classement.

Compte tenu du nombre important de retours d'information en attente, le MROS n'est pas en mesure de tirer des conclusions sur la proportion de jugements, d'ordonnances de non-entrée en matière et de décisions de classement. Il redouble donc d'efforts et cherche des solutions avec les autorités pé-

Fig. 9: Retour d'information et état concernant les dénonciations transmises au cours de l'année 2020-2024



nales afin d'obtenir les retours d'information prévus par la loi en relation avec les art. 260^{ter}, 260^{quinquies}, al. 1, 305^{bis} et 305^{ter}, al. 1, CP.

3.9 Financement du terrorisme

En 2024, le MROS a reçu 106 communications relatives à des soupçons de financement du terrorisme ou à une violation de la loi fédérale interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées³⁹, ce qui représente 0,7% de toutes les communications reçues. La plupart d'entre elles sont en outre liées à d'autres infractions préalables. Parmi les autres motifs de soupçons les plus fréquents, il y a eu notamment :

- appartenance à une organisation criminelle et terroriste⁴⁰ (25 mentions);
- escroquerie⁴¹ (9 mentions);
- violation de la loi sur les embargos⁴² (4 mentions);

³⁶ « Les autorités pénales annoncent sans délai au bureau de communication toutes les procédures pendantes en rapport avec les art. 260^{ter}, 260^{quinquies}, al. 1, 305^{bis} et 305^{ter}, al. 1, CP. Elles lui font parvenir sans délai les jugements et les décisions de non-lieu correspondants, y compris leur motivation. » (art. 29a, al. 1, LBA)

³⁷ Art. 29a, al. 2, LBA

³⁸ Cf. [Rapport annuel 2023 du MROS](#), p. 26 s.

³⁹ Loi fédérale du 12 décembre 2014 interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées, RS 122; abrogée le 1^{er} décembre 2022

⁴⁰ Art. 260^{ter} CP

⁴¹ Art. 146 CP

⁴² Art. 9, al. 2, de la loi du 22 mars 2002 sur les embargos, RS 946.231

- violation de la loi sur les stupéfiants⁴³ (3 mentions);
- recrutement, formation et voyage en vue d'un acte terroriste⁴⁴ (3 mentions);
- gestion déloyale (3 mentions)⁴⁵.

Les communications relatives à des soupçons de financement du terrorisme proviennent principalement de banques (76) et de prestataires de services de paiement (15).

En 2024, les IF ont cité le plus souvent les éléments à l'origine des soupçons ayant donné lieu à une communication suivants:

- articles de presse (36 mentions);
- surveillance des transactions (33 mentions);
- informations de tiers (26 mentions);
- transactions au comptant (24 mentions);
- incertitudes concernant l'arrière-plan économique (19 mentions).

Les 106 communications reçues en 2024 ont fait l'objet de 10 dénonciations aux autorités de poursuite pénale compétentes jusqu'au 31 décembre de la même année.

3.10 Criminalité organisée

Sur les 15 141 communications reçues par le MROS en 2024, les IF ont émis des soupçons de liens avec une organisation criminelle dans 424 cas (2,8%). La grande majorité de ces communications de soupçons proviennent du secteur bancaire (90,5%). Les IF ont indiqué les informations des médias (28,5%) et/ou la surveillance des transactions (17,2%; cf. tabl. 3) comme principaux éléments ayant déclenché la communication de soupçons.

Outre le lien présumé avec une organisation criminelle, les IF ont souvent mentionné l'escroquerie (42,9%) et/ou la corruption (8,5%) comme autres infractions préalables possibles. Les 424 communications de soupçons transmises au cours de l'exercice sous revue ont donné lieu à 33 dénonciations auprès des autorités de poursuite pénale compétentes.

3.11 Communications de soupçons en rapport avec les monnaies virtuelles

En 2024, 1799 communications de soupçons présentant un lien avec des monnaies virtuelles (AV⁴⁶; cf. Fig. 10) ont été identifiées, ce qui représente de

Tabl. 3: Fréquence des éléments à l'origine des soupçons mentionnés dans les communications en raison de liens présumés avec une organisation criminelle

Éléments à l'origine des soupçons (plusieurs réponses possibles, choix de la fréquence)	Nombre de mentions	% des communications globales
Informations des médias	121	28,5%
Surveillance des transactions	73	17,2%
Incertitudes concernant l'arrière-plan économique	59	13,9%
Informations de tiers	54	12,7%
Transactions au comptant	52	12,3%
Ouverture de relations d'affaires	36	8,5%
Informations des autorités de poursuite pénale	34	8,0%
Comptes de transit	34	8,0%
Informations internes au groupe	29	6,8%
Révision / Surveillance	20	4,7%

⁴³ Art. 19, al. 2, de la loi du 3 octobre 1951 sur les stupéfiants et les substances psychotropes (Loi sur les stupéfiants, LStup), RS 812.121

⁴⁴ Art. 260^{sexies} CP

⁴⁵ Art. 158, ch. 1 et 2, CP

⁴⁶ L'art. 4, al. 2, let. a, de l'ordonnance du 11 novembre 2015 sur le blanchiment d'argent (RS 955.01), entrée en vigueur le 1^{er} janvier 2016, a inscrit pour la première fois en Suisse la notion de monnaie virtuelle dans un acte législatif.

nouveau une augmentation par rapport à l'année précédente⁴⁷. Cette évolution pose de plus en plus de défis au MROS: les monnaies virtuelles compliquent le suivi des flux financiers et donc l'identification de l'origine des fonds et de l'ayant droit économique. Comme expliqué en détail dans le NRA relatif au risque de blanchiment d'argent et de financement du terrorisme liés aux crypto-actifs, publié au premier trimestre de 2024⁴⁸, les cryptomonnaies posent des risques accrus.

Depuis le printemps 2024, le MROS recense dans une catégorie distincte les IF qui, de par leur activité principale, comptent parmi les PSAV⁴⁹. Il peut ainsi en savoir davantage sur le comportement en ma-

tière de communication de cette catégorie d'IF (cf. tabl. 1: Communications de soupçons par secteur). Au 31 décembre 2024, 30 IF s'étaient enregistrés sous la catégorie PSAV/fintech sur goAML.

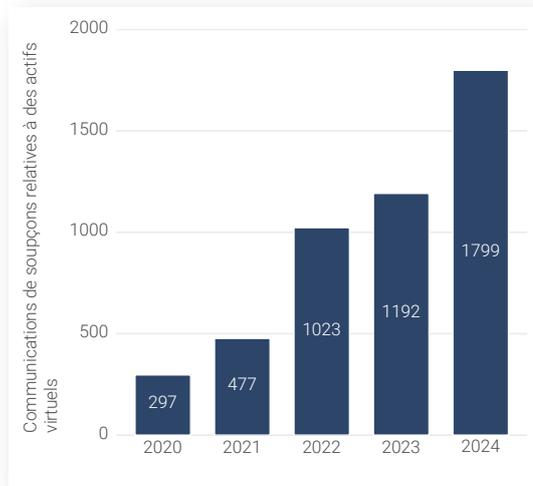
3.12 Remise d'informations au sens de l'art. 11a LBA

Alors que le MROS constatait une augmentation constante du nombre de demandes d'informations qu'il adressait à des IF en vertu de l'art. 11a LBA depuis 2020, il a enregistré une légère baisse en 2024 (1016), les valeurs retrouvant leur niveau de 2021 (cf. Fig. 11). Sur les 1016 demandes d'informations reçues, le MROS a adressé la plupart de ses demandes à des intermédiaires dits tiers. (40,7%; art. 11a, al. 2 LBA⁵⁰) qui, en plus de l'IF émetteur de la communication, prennent ou ont pris part à une transaction ou à une relation d'affaires.

Une demande d'informations sur quatre a été transmise aux intermédiaires financiers à l'origine des communications de soupçons (24,8%, art. 11a al. 1 LBA⁵¹).

Environ un tiers des demandes d'informations ont été transmises par le MROS à un intermédiaire financier sur la base de l'analyse d'informations reçues par un homologue étranger (34,5%, art. 11a, al. 2^{bis}, LBA⁵²). Depuis l'introduction de l'art. 11a al. 2^{bis} LBA en 2021, ces demandes ont pris de plus en plus d'importance par rapport aux autres demandes au titre de l'art. 11a LBA (+1,5% par rapport à l'année précédente).

Fig. 10: Nombre de communications présentant des liens avec des monnaies virtuelles (AV) 2020-2024



⁴⁷ Il n'est pas possible à ce jour de déterminer directement dans quelle mesure les transactions en monnaies virtuelles font l'objet d'un soupçon dans une communication, car ces transactions ne sont pas clairement identifiables. Les communications de soupçons présentant un lien pertinent avec les AV ont donc été identifiées, d'une part, au moyen des transactions effectuées entre les comptes affichés dans la communication et les comptes d'IF suisses ou étrangers exerçant une activité de PSAV et, d'autre part, au moyen d'une liste de mots-clés pertinents. On peut donc supposer que l'importance des cryptomonnaies dans les communications de soupçons est plutôt sous-estimée.

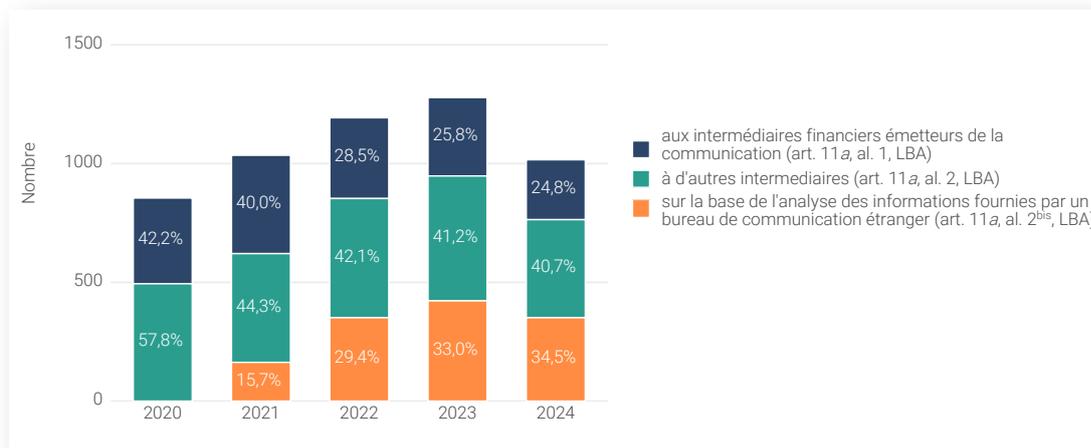
⁴⁸ Évaluation nationale des risques (National Risk Assessment, NRA) – [Risque de blanchiment d'argent et de financement du terrorisme lié aux crypto-actifs](#), janvier 2024

⁴⁹ En mars 2024, les IF enregistrés dans goAML ont été priés de communiquer au MROS s'ils pouvaient être considérés comme des PSAV de par leur activité principale.

⁵⁰ «Lorsque l'analyse montre qu'outre l'intermédiaire financier auteur de la communication, d'autres intermédiaires financiers prennent part ou ont pris part à une transaction ou à une relation d'affaires, les intermédiaires financiers concernés doivent fournir toutes les informations y afférentes au bureau de communication à la demande de ce dernier, pour autant qu'ils disposent de ces informations» (art. 11a, al. 2, LBA).

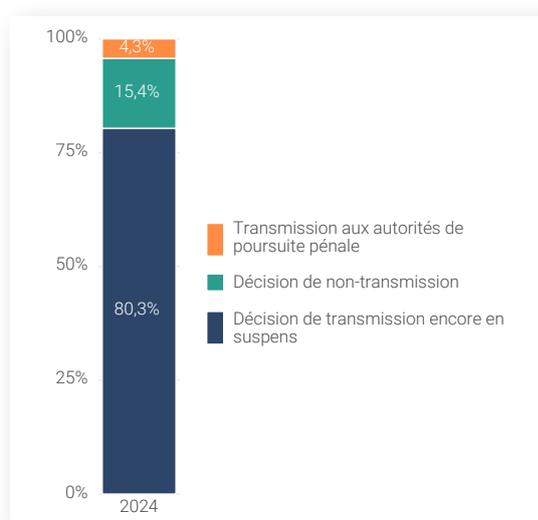
⁵¹ Si le bureau de communication a besoin d'informations supplémentaires pour analyser une communication qui lui a été transmise en vertu de l'art. 9 LBA ou de l'art. 305^{ter}, al. 2, CP, l'intermédiaire financier qui a effectué la communication doit les lui fournir sur demande, dans la mesure où il en dispose (art. 11a al. 1 LBA).

⁵² «Lorsque l'analyse des informations en provenance d'un homologue étranger montre que des intermédiaires financiers au sens de la présente loi prennent part ou ont pris part à une transaction ou à une relation d'affaires en lien avec lesdites informations, les intermédiaires financiers concernés doivent fournir toutes les informations y afférentes au bureau de communication à la demande de ce dernier, pour autant qu'ils disposent de ces informations» (art. 11a, al. 2^{bis}, LBA).

Fig. 11 : Demande de remise d'informations au sens de l'art. 11a LBA
2020-2024

3.13 Communications de rupture de la relation d'affaires au sens de l'art. 9b LBA

Depuis le 1^{er} janvier 2023, les IF peuvent, en vertu de l'art. 9b LBA⁵³, rompre la relation d'affaires 40 jours ouvrables après l'avoir signalée au MROS, pour au-

Fig. 12 : État des communications de soupçons liées à une rupture de la relation d'affaires
2024

tant que ce dernier ne leur notifie pas qu'il transmet les informations communiquées à une autorité de poursuite pénale. L'IF doit communiquer sans délai au MROS la rupture de la relation d'affaires⁵⁴.

En 2024, le MROS a reçu 7118 communications de rupture de la relation d'affaires : ce chiffre a presque triplé en comparaison avec l'année précédente (2669 en 2023). Exactement 4,3% d'entre elles se rapportent à des communications de soupçons qui ont été transmises à une autorité de poursuite pénale au cours de l'année 2024 (cf. fig. 12).

3.14 Échange d'informations avec les homologues étrangers (CRF)

Dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, le financement du terrorisme et la criminalité organisée, l'échange d'informations entre le MROS et ses homologues étrangers (les CRF) fonctionne au moyen de l'entraide administrative. Ces informations sont capitales pour les analyses effectuées par le MROS, car un grand nombre de communications de soupçons transmises par des IF suisses ont un lien avec l'étranger⁵⁵.

⁵³ En vertu de l'art. 9b LBA, les IF peuvent rompre une relation d'affaires communiquée en vertu de l'art. 9, al. 1, let. a, LBA ou de l'art. 305^{ter}, al. 2, CP pour autant que le MROS ne leur notifie pas dans un délai de 40 jours ouvrables qu'il transmet les informations communiquées à une autorité de poursuite pénale.

⁵⁴ Art. 9b, al. 3, LBA

⁵⁵ [Évaluation nationale des risques \(National Risk Assessment, NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), octobre 2021

Alors que le nombre de demandes adressées par le MROS à des CRF étrangères a augmenté ces dernières années, un léger recul est constaté en 2024. En effet, le MROS a adressé 239 demandes d'informations à 56 CRF à l'étranger (-14% par rapport à l'année précédente) et a reçu 780 demandes provenant de 96 CRF étrangères. Il a traité 422 demandes entrantes en 2024 ainsi que 188 demandes supplémentaires des l'années précédentes.

Les CRF étrangères et le MROS peuvent également échanger spontanément des informations. Il s'agit là d'un échange sans demande préalable, qu'il s'agisse d'une information de l'étranger ayant un lien avec la Suisse ou d'une information que le MROS transmet à une CRF étrangère. En 2024, le MROS a reçu 751 informations spontanées de 45 pays (726 de 53 pays en 2023) et il a envoyé 189 informations spontanées à 41 CRF étrangères (160 à 47 CRF en 2023).

3.15 Échange d'informations avec les autorités suisses

Le MROS échange également, sur demande ou spontanément, des informations pertinentes avec les autorités suisses en vertu de l'art. 29 LBA. Il s'agit d'autorités de surveillance ou d'autres autorités engagées dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme⁵⁶.

Au cours de l'exercice sous revue, le MROS a reçu 447 demandes d'informations provenant de 35 autorités suisses concernant des comptes bancaires, des personnes ou des entreprises spécifiques (696 en 2023, soit -35,8%). Comme les années précédentes, près de 80% de ces demandes émanaient d'autorités policières. Le MROS a transmis des informations spontanées aux autorités de surveillance et autres autorités suisses dans 358 cas (200 en 2023, soit +79%). En 2024, il a reçu 106 informations spontanées provenant d'autorités suisses (119 en 2023, c'est-à-dire -12,3%).

⁵⁶ Ne sont pas prises en compte dans les chiffres les demandes d'informations adressées par le MROS à d'autres autorités fédérales, cantonales et communales dans le cadre de ses analyses.

4 Tendances

Cette partie consacrée aux « Tendances » du présent rapport annuel remplace celle des « Typologies », lesquelles seront publiées sur le site Internet du MROS dès le mois de mai 2025 (cf. 2.5.2). Ces tendances donnent un aperçu global des constatations du MROS concernant certains thèmes choisis. Cette année, elles sont consacrées aux jeux d'argent en ligne, à la pédopornographie, aux actifs virtuels et à l'interdiction du Hamas.

4.1 Jeux d'argent en ligne

Généralités

La quête d'argent facile n'est pas un phénomène nouveau ou spécifique à une culture. Elle fascine les gens depuis des millénaires et constitue un comportement profondément ancré chez l'humain qui continue de jouer un rôle significatif dans le monde d'aujourd'hui⁵⁷. Si l'on interprète les chiffres, on constate un essor du marché des jeux d'argent, tant en ligne qu'en présentiel.

En 2023, le marché mondial des jeux d'argent s'est accru pour s'établir à environ 774 milliards de dollars (env. 691 milliards de francs), l'augmentation étant immense par rapport à 2006 (env. 70 milliards de dollars / 62 milliards de francs)⁵⁸. On observe une tendance haussière similaire également en Suisse : entre 2017 et 2022, le chiffre d'affaires généré par l'ensemble du secteur des jeux d'argent a progressé de 13%, passant d'environ 2,2 à 2,5 milliards de francs⁵⁹. Dans notre pays, environ six personnes sur dix ont déjà joué à des jeux d'argent au moins une fois dans leur vie⁶⁰. Le marché des jeux d'argent en ligne croît également de manière considérable. On estime que le chiffre d'affaires généré à l'échelle mondiale dans ce domaine devrait passer d'environ 85 milliards de dollars (env. 76 milliards de francs) en 2023 à 173 milliards de dollars (155 milliards de francs) en 2039⁶¹.

De nombreux États font un lien entre la hausse rapide des chiffres d'affaires, générés notamment par des activités de jeux d'argent en ligne, et le risque marqué et croissant de blanchiment d'argent. Les États-Unis⁶² observent par exemple une augmentation du risque de blanchiment d'argent liée à l'apparition de nouveaux opérateurs de plates-formes de jeux en ligne. L'évaluation nationale des risques de Malte pointe également un risque majeur dans ce domaine, eu égard notamment aux potentiels opérateurs criminels⁶³.

Compte tenu des risques croissants de blanchiment d'argent observés à l'étranger, il convient d'examiner la situation en Suisse.

Risque potentiel de blanchiment d'argent

Le risque de blanchiment d'argent peut se manifester dans une maison de jeu lors de chacune des trois phases du blanchiment (placement, dissimulation et intégration) :

- **Placement (préparation au jeu d'argent) :** les maisons de jeu échangent du liquide (monnaie fiduciaire) contre des chèques (monnaie scripturale), convertissent des coupures (smurfing). Au niveau des joueurs, l'échange en devises étrangères peut être effectué. Dans les maisons de jeu physiques, les joueurs peuvent utiliser des jetons qu'ils ont préalablement échangés directement à la table ou à la caisse, la plupart du temps contre des espèces. Des hommes de paille peuvent être employés pour dissimuler les rapports de propriété réels.
- **Dissimulation de l'origine (pendant le jeu) :** les criminels peuvent avoir de plus en plus recours aux services financiers (par ex. dépôts de la clientèle ou trafic des paiements international) des maisons de jeu. Ils sont aussi disposés à perdre une partie de leur mise pour récupérer des valeurs patrimoniales en apparence légales.

⁵⁷ Site Internet des maisons de jeu de la Saxe, [Die Geschichte des Glücksspiels](#), article du 2 novembre 2022 (en allemand), consulté le 31 janvier 2025

⁵⁸ Rapport du GAFI, [Les fragilités en termes de blanchiment de capitaux et de financement du terrorisme des casinos et du secteur des jeux, 2009, p. 9](#) (en anglais)

⁵⁹ Rapport de la Conférence spécialisée des membres de gouvernements concernés par les jeux d'argent, [Marktanteile des legalen und des illegalen Geldspielangebots in der Schweiz, Internet- und Sekundärdaten-Analyse](#), avril 2024, p. 3 (en allemand)

⁶⁰ Étude de l'Institut suisse de recherche sur la santé publique et les addictions, [Jeux d'argent : comportement et problématique en Suisse en 2022, résumé](#), Zurich, octobre 2024

⁶¹ Global Strategic Business Report, [Mobile Gambling Market Assessment and Investment Opportunities](#), septembre 2024 (en anglais)

⁶² Department of the Treasury, [2024 National Money Laundering Risk Assessment \(NMLRA\)](#), pp. 81 ss (en anglais)

⁶³ National Coordinating Committee on Combating Money Laundering and Funding of Terrorism, [Malta's National Risk Assessment 2023](#), pp. 115 ss (en anglais)

- **Phase d'intégration** : pour pouvoir blanchir des fonds à grande échelle par le biais des jeux d'argent, les criminels visent l'exploitation de maisons de jeu, notamment à l'étranger⁶⁴.

Situation en matière de risque et législation en Suisse

Selon les rapports sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse publiés en 2015⁶⁵ et en 2021⁶⁶, le risque de blanchiment d'argent dans le secteur des jeux d'argent est considéré comme très faible. Le rapport de 2021 ajoute que le risque lié aux maisons de jeu en ligne suisses, qui ne sont exploitées que depuis 2019, est difficile à mesurer.

Les conditions strictes d'octroi d'une concession, laquelle est requise en Suisse pour exploiter une maison de jeu (casino), pourraient expliquer le risque faible de blanchiment d'argent. À compter de fin 2024, le Conseil fédéral a attribué, pour la période de 2025 à 2044, dix concessions sans restriction légale des gains maximaux⁶⁷ et douze avec limitation⁶⁸, soit 22 concessions au total⁶⁹. L'attribution des concessions est assortie de critères de vérification stricts. Le requérant et toutes les autres personnes impliquées doivent jouir d'une bonne réputation⁷⁰ et pouvoir garantir une activité commerciale irréprochable. De plus, ils doivent être en mesure de démontrer que les requérants disposent d'un programme de mesures de sécurité suffisant

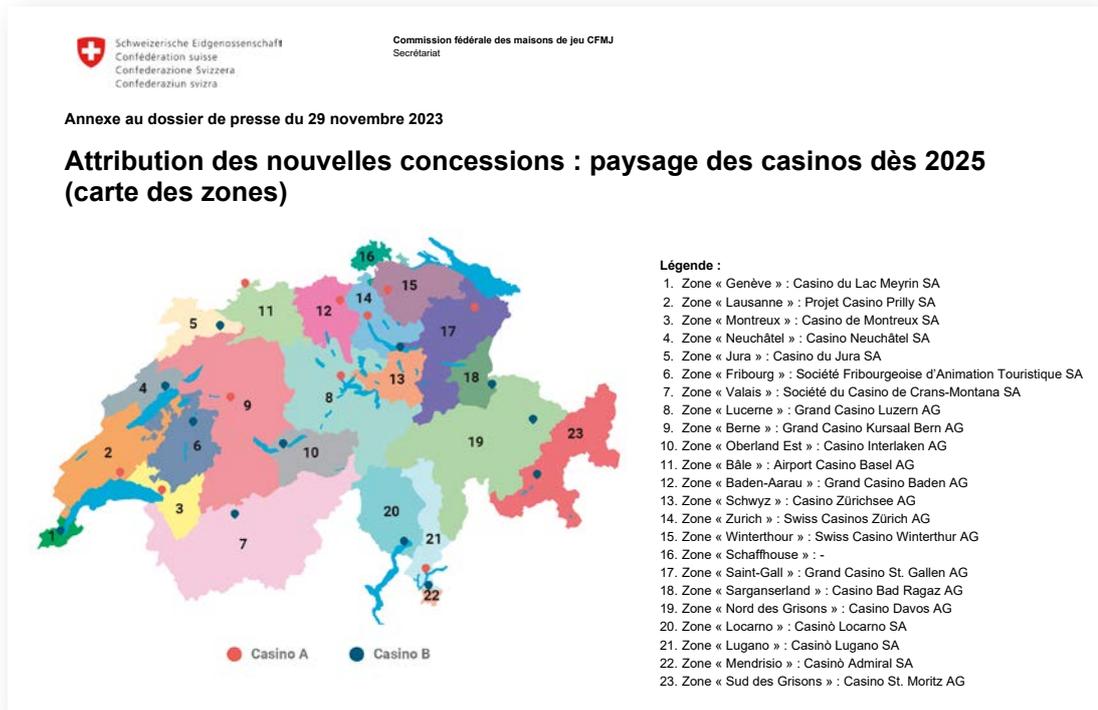


Fig. 13: Commission fédérale des maisons de jeu (CFMJ), Attribution des nouvelles concessions : paysage des casinos dès 2025 (carte des zones), novembre 2023.

⁶⁴ [Première évaluation nationale des risques \(NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), juin 2015, p. 87

⁶⁵ Ibid., p. 5

⁶⁶ [Deuxième évaluation nationale des risques \(NRA\) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), octobre 2021, p. 45

⁶⁷ Concession de type A

⁶⁸ Concession de type B

⁶⁹ Communiqué de presse du Conseil fédéral du 29 novembre 2023: [Le Conseil fédéral attribue les concessions pour les maisons de jeu : continuité dans le paysage des casinos](#)

⁷⁰ Message du 21 octobre 2015 concernant la loi fédérale sur les jeux d'argent, FF 2015 7627, 7678: « À cet égard, le comportement passé de ces personnes sur le marché suisse constituera un critère important. Ainsi, on doit par exemple partir de l'idée que celui qui aurait, par le passé, exploité de manière ciblée le marché suisse des jeux de casino en ligne sans autorisation, voire aurait fait l'objet d'une condamnation entrée en force – en Suisse ou à l'étranger –, ne remplira pas le critère de la bonne réputation selon le nouveau droit. »

pour lutter contre la criminalité et le blanchiment d'argent⁷¹.

Depuis le 1^{er} janvier 2019, la LJA^r donne la possibilité aux maisons existantes d'exploiter des jeux de casino en ligne⁷². Pour ce faire, le Conseil fédéral doit toutefois leur octroyer une extension de concession. Une fois au bénéfice de cette extension de concession, les casinos doivent encore obtenir les autorisations nécessaires pour les divers jeux proposés de la part de la CFMJ avant de pouvoir débiter leur activité en ligne⁷³. Ils doivent en outre respecter les obligations de diligence prévues par la LBA afin de lutter contre le blanchiment d'argent. Dix requérants ont obtenu une telle autorisation en Suisse pour la nouvelle période à compter de 2025⁷⁴.

Lorsque la demande de concession est examinée, l'accent est mis sur l'identification précoce de potentiels opérateurs à risque afin de les exclure avant même de leur attribuer une concession. S'ils exploitent une concession également, les opérateurs sont tenus de respecter les prescriptions en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.⁷⁵ Ils doivent ainsi veiller aux obligations de diligence prévues par la LBA lors de l'ouverture d'un compte de joueur pour un jeu d'argent en ligne ou procéder à des clarifications lorsque des transactions sont effectuées par le biais de ce compte⁷⁶. L'attention est donc portée sur le joueur lorsqu'une concession est exploitée.

Dans notre pays, seuls sont autorisés les opérateurs disposant d'une concession suisse. Les opérateurs étrangers qui proposent leurs jeux en ligne sans concession suisse sont interdits. La CFMJ bloque les sites Internet qui ne respectent pas cette règle et les inscrit sur sa liste des offres de jeux en ligne non autorisées⁷⁷.

Comportement en matière de communication en Suisse

Le niveau des communications de soupçons provenant de maisons de jeu suisses est faible depuis plus de dix ans. Entre 2014 et 2024, les maisons de jeu ont transmis en moyenne 0,5% du total des communications. En 2024, cette valeur s'est établie à 0,3% (47 communications de soupçons sur 15 141 ; cf. tabl. 1).

S'agissant des communications de soupçons reçues en 2024, la plupart des clarifications de fond effectuées concernant l'origine des valeurs patrimoniales utilisées pour jouer ont été déterminantes. On a ainsi constaté que des joueurs avaient par exemple acheté des jetons dans des casinos physiques avec des fonds potentiellement incriminés, n'avaient ensuite que peu joué et s'étaient fait rembourser les jetons avant de quitter le casino.

D'autres communications de soupçons avaient comme point de départ des clarifications en lien avec la protection des joueurs. Ceux-ci doivent par exemple être protégés contre la perte de contrôle sur leur jeu d'argent et empêchés de continuer à jouer pour éviter des pertes financières. Dans ces cas, les maisons de jeu sont tenues de prononcer des mesures d'exclusion lorsqu'elles savent ou présument qu'une personne est surendettée ou ne parvient plus à remplir ses obligations financières⁷⁸. Lors de la vérification des conditions de blocage, il peut par exemple être constaté que le joueur n'est pas en mesure de justifier le montant des fonds utilisés pour jouer ni leur provenance. Ces circonstances incitent les casinos à procéder à des obligations de diligence particulières et, le cas échéant, à adresser une communication de soupçon au MROS.

⁷¹ Art. 8 de la loi fédérale du 29 septembre 2017 sur les jeux d'argent (LJA^r; RS 935.51)

⁷² Art. 9 LJA^r

⁷³ CFMJ, [Maisons de jeu en ligne](#), consulté le 31 janvier 2025

⁷⁴ Ibid., consulté le 31 janvier 2025

⁷⁵ Art. 67 ss. LJA^r et Ordonnance de la Commission fédérale des maisons de jeu concernant les obligations de diligence des maisons de jeu en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (Ordonnance de la CFMJ sur le blanchiment d'argent, OBA-CFMJ), RS 955.021.

⁷⁶ Art. 52 en relation avec l'art. 47 de l'ordonnance du 7 novembre 2018 sur les jeux d'argent (OJA^r; RS 935.511). Il convient également de mentionner les autres dispositions légales visant à lutter contre le blanchiment d'argent, notamment l'interdiction faite aux maisons de jeu de délivrer des attestations de gains (art. 70 LJA^r) et les prescriptions supplémentaires relatives aux chèques et aux dépôts (art. 69 LJA^r).

⁷⁷ CFMJ, [Jeux en ligne non autorisés](#), consulté le 31 janvier 2025

⁷⁸ Office fédéral de la santé publique (OFSP), [Jeux d'argent](#), consulté le 31 janvier 2025

Dans les casinos étrangers, l'utilisation de cryptomonnaies est une question brûlante qui n'a pas encore touché la Suisse. En Suisse, les cryptomonnaies sont actuellement interdites comme moyen de paiement⁷⁹.

Les conclusions tirées de la poursuite pénale dressent un tableau homogène s'agissant du nombre de cas communiqués : seuls quelques jugements ont été prononcés en lien avec le blanchiment d'argent dans des casinos suisses et les sommes impliquées étaient généralement modestes. Le détenteur d'un compte de joueur (X) a été condamné le 21 juillet 2023 à une peine pécuniaire par ordonnance pénale rendue par le ministère public du canton de Zoug en vertu de l'art. 305^{bis}, al. 1, CP. Selon le jugement, d'autres personnes utilisaient le compte de X au su de ce dernier pour jouer dans un casino en ligne. Une autre personne (Y) en a profité pour utiliser le compte de X afin de jouer avec des fonds générés illégalement. Y s'était procuré les données bancaires d'une troisième personne (Z) pour verser de l'argent depuis le compte de cette dernière sur le compte de joueur de X. X versait sur son compte bancaire les gains générés par Y, les retirait en espèces et les donnait ensuite à Y.

Globalement, on peut dire que le blanchiment d'argent dans les maisons de jeu est combattu à plusieurs niveaux en Suisse, notamment par l'obligation de concession des opérateurs et les mesures imposées aux joueurs découlant de la législation sur le blanchiment d'argent, qui sont strictes par rapport à l'étranger. De plus, les mai-

sons de jeu en ligne étrangères non autorisées sont bloquées et inscrites sur la liste de la CFMJ correspondante. Le dispositif de lutte est donc efficace en Suisse, raison pour laquelle le MROS reçoit peu de communications concernant les jeux d'argent en ligne.

4.2 Pédopornographie et actifs virtuels

Chaque année, la Statistique policière de la criminalité (SPC) recueille les chiffres sur la pornographie illicite visée à l'art. 197 CP, qui battent à chaque fois de nouveaux records⁸⁰. Cette statistique ne permet toutefois pas de connaître le nombre d'infractions concernant explicitement la pédopornographie. Bien que les autorités de poursuite pénale aient engrangé quelques succès contre les milieux de la pornographie⁸¹, leur tâche dans ce domaine s'avère compliquée⁸². En raison de la connectivité numérique, les victimes et les criminels se trouvent rarement dans le même pays. La SPC⁸³ dresse le même constat : en effet, même si l'abus est commis au niveau local, les images et les vidéos sont diffusées et consommées à l'échelle mondiale. En 2023, on a recensé 2967 infractions en lien avec de la pornographie en Suisse⁸⁴, dont 85,4% ont été commises en ligne⁸⁵.

La pédopornographie est punissable en vertu de l'art. 197 CP. S'il y a élément constitutif d'infraction au sens de l'art. 197, al. 4, CP⁸⁶, une peine privative de liberté de cinq ans au plus est encourue. Il s'agit donc d'un crime qui constitue une infraction préalable au blanchiment d'argent⁸⁷.

⁷⁹ Évaluation nationale des risques – National Risk Assessment (NRA) – [Rapport Risque de blanchiment d'argent et de financement du terrorisme lié aux crypto-actifs](#), janvier 2024, p. 38

⁸⁰ Office fédéral de la statistique (OFS), [Code pénal \(CP\) : infractions pénales et personnes prévenues, 2009-2023](#)

⁸¹ SRF News, [Ermittlungen in Deutschland – Grosse Kinderpornografie-Plattform abgeschaltet](#) (en allemand), consulté le 31 janvier 2025; Blick, [Koordinierte Aktion im Tessin – Zwölf Menschen wegen illegaler Pornografie festgenommen](#) (en allemand), consulté le 31 janvier 2025

⁸² Neue Zürcher Zeitung (NZZ), [Kinderporno-Flut: Ermittler aus Zürich sagt, es werde immer schlimmer](#) (en allemand), consulté le 31 janvier 2025

⁸³ OFS, [Statistique policière de la criminalité \(SPC\) – Rapport annuel 2023 des infractions enregistrées par la police](#)

⁸⁴ Ibid., p. 9

⁸⁵ Ibid., p. 62

⁸⁶ Quiconque fabrique, importe, prend en dépôt, met en circulation, promeut, expose, offre, montre, rend accessible, met à disposition, acquiert, obtient par voie électronique ou d'une autre manière ou possède des écrits, enregistrements sonores ou visuels, images ou autres objets pornographiques ou des représentations pornographiques ayant comme contenu des actes d'ordre sexuel effectifs avec des mineurs peut être condamné à une peine privative de liberté de cinq ans au plus ou à une peine pécuniaire en vertu de l'art. 197, al. 4, 2^e phrase, CP.

⁸⁷ Sont considérés comme des infractions préalables au blanchiment d'argent les crimes, c'est-à-dire les infractions passibles d'une peine privative de liberté de plus de trois ans (cf. art. 305^{bis}, ch. 1, en relation avec l'art. 10, al. 2, CP).

Compte tenu du fait que l'infraction de pédopornographie est principalement commise en ligne et que les contenus concernés font régulièrement l'objet de paiements, il est d'autant plus étonnant que le MROS n'ait réceptionné aucune communication de soupçons de pédopornographie en 2024. En revanche, il a reçu de la part de CRF étrangères 70 informations spontanées qui ont permis, dans quelques cas, d'établir des liens avec des communications de soupçons pour lesquelles les IF n'avaient pas été en mesure d'identifier clairement l'infraction préalable au blanchiment d'argent.

Les CRF étrangères ont communiqué au MROS le nom de criminels potentiels qui ont principalement utilisé des portefeuilles de cryptomonnaie et d'autres moyens de paiement présumément anonymes pour envoyer de faibles montants à des complices ou les verser sur des comptes et des portefeuilles à l'étranger. Ces constats concordent avec les résultats de l'étude menée par l'ONG Internet Watch Foundation (IWF). Celle-ci rapporte que des cryptomonnaies, des cartes de crédit et des sociétés de transfert de fonds sont principalement utilisées pour payer du matériel relatif à des abus sexuels sur des enfants (child sexual abuse material, CSAM)⁸⁸. Les IF auteurs des communications à l'étranger sont parvenus à démontrer un lien clair entre les portefeuilles utilisés, les comptes ou les criminels potentiels et l'infraction. Les adresses des criminels sont réparties sur tout le territoire suisse; il n'existe pas de point névralgique. En revanche, les victimes se trouvent majoritairement en Asie, en Europe de l'Est et en Amérique du Sud.

En fin de compte, ni la pédopornographie ni les modes de paiement virtuels ne sont des phénomènes nouveaux. On constate cependant une disparité entre l'absence de communications émanant d'IF suisses et les informations spontanées régulièrement reçues de l'étranger. Le MROS s'engage donc pour combler cette lacune, notamment depuis qu'il a rejoint en 2024 le groupe de travail « Sexual Child Abuse » au

sein de l'Europol Financial Intelligence Public Private Partnership (EFIPPP). Il tire parti des informations obtenues dans ce cadre pour sensibiliser les IF (par ex. le guide FIAHT; cf. ch. 2.5.1)⁸⁹.

Dans la mesure du possible, les IF sont tenus de transmettre une communication de soupçons en indiquant l'infraction préalable présumée dès qu'ils identifient un indicateur. C'est la seule manière de garantir une analyse correcte et ciblée de la communication par le MROS, même en l'absence d'informations complémentaires de l'étranger, puis sa transmission aux autorités de poursuite pénale.

4.3 Interdiction du Hamas

La LBA impose aujourd'hui déjà aux IF et aux négociants l'obligation de communiquer au MROS en lien avec le financement du terrorisme, notamment s'ils savent ou ont des soupçons fondés indiquant que les valeurs patrimoniales impliquées dans la relation d'affaires ont un rapport avec une infraction prévue à l'art. 260^{ter} CP (organisations criminelles et terroristes)⁹⁰, sont soumises au pouvoir de disposition d'une organisation criminelle ou terroriste⁹¹ ou servent au financement du terrorisme⁹².

L'un des défis auquel sont confrontés les IF consiste à identifier le financement du terrorisme car les fonds sont souvent « propres », c'est-à-dire non incriminés. Dans ce cas, et contrairement à un soupçon de blanchiment d'argent, l'IF ne doit pas vérifier si les valeurs patrimoniales proviennent d'une infraction préalable au blanchiment d'argent, mais plutôt si elles pourraient servir à l'avenir au financement du terrorisme. Cette tâche est évidemment difficile, notamment lorsque les valeurs patrimoniales sont transmises à des personnes ou à des organisations qui n'ont aucun lien direct avec des organisations terroristes connues et dont les activités n'ont jusqu'ici pas été qualifiées de terroristes. Il est donc plus ardu d'identifier et de combattre le financement du terrorisme avant le passage à l'acte

⁸⁸ [Internet Watch Foundation, The Annual Report 2022](#), p. 85 (en anglais)

⁸⁹ Cf. par ex. les indicateurs d'identification de pédopornographie mentionnés dans le guide FIAHT publié par le MROS [Financial Intelligence against Human Trafficking Guide](#), pp. 15 et 19 ss.

⁹⁰ Cf. art. 9, al. 1, let. a, ch. 1, LBA.

⁹¹ Cf. art. 9, al. 1, let. a, ch. 3, LBA.

⁹² Cf. art. 9, al. 1, let. a, ch. 4, LBA.

que de se baser sur des faits passés (comme c'est le cas pour le blanchiment d'argent). À cela s'ajoute le fait que les montants impliqués dans le financement du terrorisme sont souvent minimes (dons de plusieurs personnes), passent sous le radar du suivi (automatique) des transactions mené par les IF et ne donnent donc lieu à aucune analyse approfondie⁹³.

Le 4 septembre 2024, le Conseil fédéral a adopté le message sur la loi fédérale interdisant le Hamas et les organisations apparentées et l'a transmis au Parlement⁹⁴. En décembre 2024, l'Assemblée fédérale a décidé d'adopter la loi fédérale⁹⁵. Le Conseil fédéral fixera la date d'entrée en vigueur après l'expiration du délai référendaire (19 avril 2025). En outre, le Conseil fédéral a été chargé d'interdire le Hezbollah. L'interdiction est gage de sécurité juridique pour les IF car ces derniers ne doivent plus évaluer eux-mêmes si le Hamas et les organisations apparentées sont des organisations terroristes. Cette qualification d'organisation terroriste apporte, également pour le MROS, une clarté qui permet de déterminer de manière univoque une infraction préalable au blanchiment d'argent⁹⁶ et constitue la base de l'échange d'informations avec les autorités partenaires étrangères. Si les IF envoient un nombre plus élevé de communications de soupçons concernant le financement du terrorisme, davantage d'informations pourront être échangées avec l'étranger par la voie de l'entraide administrative internationale, ce qui renforcera de fait l'efficacité de la poursuite pénale.

Depuis l'attaque du Hamas contre Israël du 7 octobre 2023, le MROS a reçu une quarantaine de communications de soupçons liées au financement potentiel du Hamas. Sur le lot de communications, le MROS a constaté des risques relatifs aux associations et fondations soutenant a priori des projets humanitaires. Les déclarations publiques « pro-Hamas » de certains membres de ces institu-

tions ont amené le MROS à analyser de manière approfondie le financement de ces personnes morales et les sorties de fonds. Les déclarations publiques « pro-Hamas » de personnes privées qui reçoivent des dons et retirent l'argent en espèces ont également amené le MROS à analyser de manière approfondie plusieurs cas. En ce qui concerne les cryptomonnaies, certains IF actifs dans ce secteur se sont adonnés à des analyses de transactions sur la blockchain. Des liens, souvent indirects, avec des wallets flagés ont donné lieu à des communications de soupçons.

Le MROS tient à avoir une vision d'ensemble sur de potentiels financements du Hamas depuis la Suisse. Les cas où le soupçon de financement d'une organisation terroriste est fondé sont transmis au MPC.

En résumé, l'entrée en vigueur de la loi fédérale interdisant le Hamas et les organisations apparentées crée une sécurité juridique grâce à la qualification du Hamas en tant qu'organisation terroriste. Le MROS suit en permanence l'évolution de la situation concernant les communications qu'il reçoit en lien avec le Hamas. Il observe que des associations et fondations apportant un soutien financier à des projets humanitaires présentent un risque potentiel de financement du terrorisme (cf. courrier de sensibilisation et typologies à l'attention des IF)⁹⁷.

⁹³ Deuxième évaluation nationale des risques (NRA) – Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, octobre 2021, p. 48

⁹⁴ Communiqué de presse du Conseil fédéral du 4 septembre 2024 : [Le Conseil fédéral adopte le message sur la loi fédérale interdisant le Hamas](#)

⁹⁵ Texte soumis au vote final le 20 décembre 2024, FF 2025 21.

⁹⁶ Sont considérés comme des infractions préalables au blanchiment d'argent les crimes, c'est-à-dire les infractions passibles d'une peine privative de liberté de plus de trois ans.

⁹⁷ Alerte du 3 novembre 2023 et addendum du 5 décembre 2023 : cette alerte se composait des publications du GAFI ainsi que d'informations de CRF étrangères et du MROS ; disponible sur [Publications du Bureau de communication en matière de blanchiment d'argent \(MROS\)](#)

5 Pratique du MROS

5.1 Immédiateté vs degré de clarification des communications – Position du MROS

Ces deux dernières années, le MROS a constaté des déficiences et des niveaux de qualité variables concernant le contenu des communications de soupçons. Il arrive parfois que les établissements financiers ne transmettent plus que des informations très rudimentaires ou des faits à peine clarifiés. Ou alors le MROS ne peut pas déterminer avec certitude si les obligations de diligence particulières prévues à l'art. 6 LBA ont été observées et les éléments de soupçon concrètement traités. Il avait déjà souligné cette évolution dans son rapport annuel 2023 et l'avait expliquée par la pression générale exercée sur les coûts. De plus, les IF font valoir qu'ils sont mis encore plus sous pression qu'auparavant pour transmettre une communication aussi rapidement que possible. Ils estiment que les autorités ont durci la notion d'« immédiateté », qui définit le délai dans lequel une communication doit être transmise au MROS. La menace d'une procédure pénale pour les IF et leurs collaborateurs accroît massivement la pression.

Le MROS ne peut prendre position sur cette déclaration qu'en ce qui concerne son domaine central, soit le système de communication opérationnel. Le dispositif suisse de lutte contre le blanchiment d'argent repose sur le fait que l'IF procède aux premières clarifications de base concernant d'éventuelles valeurs patrimoniales ou transactions illégales. Le législateur s'est prononcé clairement en faveur d'un système de communication qualitatif. Actuellement, le droit suisse ne prévoit délibérément pas de communications « basées sur des seuils », qui nécessiteraient par exemple un certain montant de transaction ou un autre élément quantitatif déterminant. Les obligations de diligence inscrites dans la LBA suivent une organisation en cascade et répétitive. Elles ont pour point de départ les art. 3 à 5 LBA, à savoir la vérification de l'identité du cocontractant, l'identification de l'ayant droit économique et la répétition périodique de ces obligations. Les obligations de diligence particulières au sens de l'art. 6 LBA prévoient que l'arrière-plan et le but d'une transaction ou d'une relation d'affaires doivent être examinés en fonction des risques. Les

IF doivent creuser les indices et les éléments suspects et les clarifier en bonne et due forme. C'est uniquement lorsque ces clarifications ne sont pas concluantes, c'est-à-dire que les éléments suspects ne peuvent pas être écartés et qu'un soupçon fondé se manifeste, qu'ils peuvent informer le MROS en vertu de l'art. 9 LBA. Ce « programme d'examen » présuppose que les IF puissent prendre le temps nécessaire pour effectuer les clarifications requises dans un degré adéquat. Le temps consacré varie d'un cas à un autre en fonction du risque, des faits et de la complexité de la relation d'affaires. L'IF a besoin d'une certaine marge de manœuvre pour choisir sa manière de clarifier le cas et le délai requis pour ce faire. Par conséquent, il n'est pas possible de généraliser la durée correcte ou appropriée que nécessitent les clarifications. Cette durée varie en fonction du cas concret. Néanmoins, les clarifications visent à ce que l'IF examine les faits en profondeur et se forge une opinion fondée.

Les communications de soupçons et les clarifications sous-jacentes doivent présenter une certaine qualité matérielle pour que le MROS puisse les traiter judicieusement. Les faits rudimentaires ou non clarifiés rendent l'analyse compliquée voire impossible. De telles communications de soupçons bloquent le système d'information et requièrent des ressources inutiles au MROS. Elles ont un effet néfaste sur l'efficacité du traitement des communications et affaiblissent globalement le dispositif de lutte contre le blanchiment d'argent.

Depuis l'introduction de l'approche de traitement basée sur les risques, le MROS abandonne peu à peu la stratégie de traitement traditionnelle selon laquelle une communication équivaut à une dénonciation auprès des autorités de poursuite pénale au profit du renseignement actif et de la mise en réseau des informations. Ce n'est plus la communication de soupçons en tant que telle qui est au centre de l'analyse⁹⁸, mais son contenu informatif. Cette analyse se fonde sur des faits substantiels ayant été clarifiés de la manière la plus exhaustive possible. Ces facteurs influent davantage sur l'efficacité que le facteur temporel. Le degré de clarification ne doit pas être sacrifié sur l'autel de l'immédiateté.

⁹⁸ Cf. [Rapport annuel 2023 du MROS](#), ch. 2.3.

L'exhaustivité des communications de soupçons est aussi importante qu'un degré suffisant de clarification. Le MROS continue de recevoir de nombreuses communications qui contiennent des données insuffisantes ou incomplètes. Il doit les renvoyer pour correction aux IF à moins que ses collaborateurs ne puissent les corriger manuellement, ce qui nécessite toutefois à nouveau des ressources⁹⁹. Lorsqu'elle est renvoyée à un IF, la communication ne peut pas être traitée. En toute logique, le MROS n'envoie une confirmation de réception aux IF conformément à l'art. 4 OBCBA qu'après avoir reçu une communication complète et correcte.

Tant le degré de clarification sur le plan matériel qu'une documentation complète et structurée des communications de soupçons transmises au MROS sont essentiels au traitement efficace des communications et au soutien des autorités de poursuite pénale dans la lutte contre le blanchiment d'argent.

5.2 Interprétation de l'art. 11a LBA – Justification des demandes de renseignements

L'art. 11a LBA donne la possibilité au MROS de demander des informations aux IF lorsque l'analyse des communications effectuée en vertu de l'art. 9 LBA ou 305^{er} al. 2 CP ou sur la base d'informations fournies par des CRF étrangères permet d'établir que les IF concernés ont participé aux faits par le biais de transactions ou de relations d'affaires. Les demandes de renseignements adressées par le MROS aux IF visent, d'une part, à replacer les communications de soupçons reçues dans un contexte plus large et, d'autre part, à fournir aux CRF étrangères les informations nécessaires à la lutte contre le blanchiment d'argent et le financement du terrorisme (cf. à ce sujet le rapport annuel 2023 du MROS, ch. 6.1). Cette possibilité de recueillir des informations est l'un des principaux instruments du MROS pour lutter efficacement contre le blanchiment d'argent et le financement du terrorisme.

Les communications de soupçons en vertu de l'art. 9 LBA ou 305^{er}, al. 2, CP et les informations des CRF étrangères reçues par le MROS contiennent une quantité importante de données personnelles et financières, dont certaines sont sensibles. Le MROS est tenu de respecter les dispositions légales en matière de protection des données. Cela concerne également les informations qu'il utilise et divulgue lorsqu'il rédige des demandes de renseignements à l'attention des IF en vertu de l'art. 11a LBA.

Le cadre légal suisse prévoit des dispositions d'ampleurs diverses visant à garantir la protection des données et, plus spécifiquement, des informations relatives à des communications de soupçons, la principale de ces dispositions étant l'art. 320 CP, qui punit la violation du secret de fonction. Par ailleurs, les art. 9 et 10a LBA disposent que les communications de soupçons transmises au MROS doivent être traitées de manière strictement confidentielle. En d'autres termes, les IF doivent garder secrètes les informations concernant des transactions suspectes pour ne pas compromettre les enquêtes potentielles.

La LBA ne prévoit pas qu'il faille motiver une demande de renseignements adressée aux IF. Par conséquent, le MROS n'est par exemple pas autorisé à divulguer le motif (de soupçon) pour lequel une analyse est en cours, ni le lien entre un client et une communication de soupçons. Cette approche vise aussi à empêcher les IF de sélectionner les informations demandées, d'autant plus qu'ils sont tenus de transmettre toutes les informations sollicitées par le MROS (cf. à ce sujet le rapport annuel 2023 du MROS, ch. 6.1).

Conformément à sa pratique, le MROS ne justifie donc pas les demandes de renseignements qu'il adresse aux IF. Seules les informations sur la relation d'affaires qui permettent aux IF d'identifier cette dernière ou le titulaire de la relation sont sollicitées et divulguées: par exemple le numéro de compte, l'IBAN ou le nom.

⁹⁹ Cf. [Rapport annuel 2023 du MROS](#), ch. 3.

Lorsqu'il demande des renseignements, le MROS ne fournit pas d'explications supplémentaires sur les raisons pour lesquelles les informations sont sollicitées et sur le contexte dans lequel elles s'inscrivent. S'il le faisait, les IF concernés pourraient avoir connaissance de l'analyse en cours auprès du MROS, ce qui pourrait entraîner un risque de collusion. Néanmoins, en demandant des renseignements en vertu de l'art. 11a, al. 2 et 2^{bis}, LBA, le MROS dévoile implicitement qu'il effectue des analyses sur le ou les clients d'un intermédiaire financier. Les IF peuvent donc supposer qu'il a reçu une communication de soupçons ou une demande de l'étranger concernant l'un de leurs clients. Par ailleurs, le MROS n'est pas autorisé à partager des informations avec les IF, au risque de violer son secret de fonction.

5.3 Obligation de communiquer et droit de communiquer

Le droit de communiquer et l'obligation de communiquer visés respectivement aux art. 305^{ter}, al. 2, CP et 9 LBA coexistent dans le système suisse de communication de soupçons. En vigueur depuis le 1^{er} août 1994, le droit de communiquer a été mis en œuvre comme motif justificatif légal afin que les IF ne s'exposent pas au risque d'une violation de leur secret professionnel. La base légale relative à l'obligation de communiquer est la LBA, qui est entrée en vigueur le 1^{er} avril 1998.

Au moment de l'entrée en vigueur de la LBA, la question se posait déjà de savoir s'il fallait que le droit de communiquer et l'obligation de communiquer coexistent. Cette question s'est reposée dans le cadre du projet du Secrétariat d'État aux questions financières internationales (« projet SFI »)¹⁰⁰ et de l'introduction de l'art. 9, al. 1^{quater}, LBA, qui définit et inscrit dans la loi l'élément déterminant l'obligation de communiquer, à savoir le soupçon fondé. À l'époque, le Conseil fédéral proposait de supprimer le droit de communiquer au profit de l'obligation de communiquer. Il mentionnait dans son rapport ex-

plicatif sur le projet soumis à consultation¹⁰¹ que le droit de communiquer prévu à l'art. 305^{ter}, al. 2, CP n'était plus guère applicable selon la législation en vigueur. En effet, si on considère la jurisprudence, l'état de fait visé par le droit de communiquer tombe déjà en grande partie sous l'obligation de communiquer de l'art. 9 LBA. Il s'ensuit que, tant en cas de communication selon l'art. 9 LBA que selon l'art. 305^{ter}, al. 2, CP, les conséquences sont les mêmes: les fonds ne sont pas bloqués automatiquement. En outre, en cas de transmission du cas aux autorités de poursuite pénale par le MROS, les deux types de communication ont les mêmes conséquences, à savoir le blocage des valeurs patrimoniales confiées pendant cinq jours.

Lors de la consultation relative au projet SFI, le secteur a fortement critiqué la suppression du droit de communiquer. Il craignait que les collaborateurs des IF s'exposent davantage au risque de punissabilité pour violation du secret bancaire¹⁰². On peut répondre à cette crainte que tant l'art. 305^{ter}, al. 2 CP que l'art. 11 LBA contiennent un motif justificatif légal suffisant. Toutefois, en raison des critiques émises à l'époque, le droit de communiquer n'a pas été supprimé. Dans son message, le Conseil fédéral considérait le droit de communiquer comme un instrument subsidiaire à l'obligation de communiquer. Lorsqu'il exerce son droit de communiquer, l'IF est également tenu d'effectuer les clarifications découlant des obligations de diligence particulières visées à l'art. 6, al. 2, LBA. Le droit de communiquer ne peut être utilisé pour annoncer des cas au MROS sans effectuer aucune clarification au préalable. Le Conseil fédéral estimait que, en raison du nouveau libellé de l'art. 9, al. 1^{quater}, LBA et de l'interprétation large de la notion de « soupçon fondé », la proportion de communications de soupçons basées sur le droit de communiquer diminuerait au profit des communications sur la base de l'obligation de communiquer¹⁰³.

Les statistiques (cf. ch. 3.4) illustrent que les communications adressées sur la base du droit de

¹⁰⁰ RO 2021 656, cf. aussi le [message du 26 juin 2019 concernant la modification de la loi sur le blanchiment d'argent](#), FF 2019 5237, 5263 ss.

¹⁰¹ [Modification de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme – Rapport explicatif sur le projet soumis à consultation](#)

¹⁰² Cf. [Rapport de résultats du 26 juin 2019 sur la consultation relative à la modification de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme \(loi sur le blanchiment d'argent\)](#), ch. 8.1.1.

¹⁰³ [Message du 26 juin 2019 concernant la modification de la loi sur le blanchiment d'argent](#), FF 2019 5237, 5265

communiquer ont fortement diminué en 2023. Un léger recul a été enregistré en 2024 également. Par conséquent, la question se pose à nouveau aujourd'hui : la coexistence du droit de communiquer et de l'obligation de communiquer se justifie-t-elle encore ?

Dans son analyse, le MROS ne fait pas de distinction entre les communications reçues sur la base du droit de communiquer et de l'obligation de communiquer. Il constate cependant que les IF procèdent parfois à des clarifications moins approfondies lorsqu'ils se basent sur le droit de communiquer et que les informations transmises ne sont pas assez pertinentes pour confirmer un soupçon. Le MROS rappelle que l'exercice du droit de communiquer ne libère pas les IF de leurs obligations de diligence.

5.4 Définition des « autorités de poursuite pénale »

En vertu de l'art. 23, al. 4, LBA, le MROS dénonce les cas aux autorités de poursuite pénale compétentes lorsque l'analyse d'une ou de plusieurs communications lui a permis de fonder ses soupçons. Conformément à sa pratique actuelle, il transmet ces cas aux autorités de poursuite pénale cantonales ou au MPC. Par ailleurs, d'autres autorités sont qualifiées d'autorité de poursuite pénale, en l'occurrence la Police judiciaire fédérale, les polices cantonales et les autorités disposant d'un service de droit pénal et luttant également contre les infractions préalables au blanchiment d'argent au sens de la législation ad hoc. Toutefois, le MROS ne leur transmet que des informations spontanées dans le cadre de l'entraide administrative. Aussi, la question se pose de savoir s'il pourrait dénoncer certains cas également à ces autres autorités de poursuite pénale en plus des informations spontanées qu'il leur fournit déjà.

L'art. 12 du code de procédure pénale du 5 octobre 2007 (CPP)¹⁰⁴ dresse la liste des autorités de poursuite pénale, à savoir la police, le ministère public et les autorités pénales compétentes en matière de contraventions. Ces dernières ne participent pas à

la lutte contre le blanchiment d'argent et les infractions préalables au blanchiment d'argent, contrairement à la police, qui peut également enquêter en toute autonomie sur des infractions de sa propre initiative ou sur dénonciation (art. 15, al. 2, CPP).

L'organisation des autorités pénales de la Confédération est régie par la loi du 19 mars 2010 sur l'organisation des autorités pénales (LOAP)¹⁰⁵. Conformément à l'art. 2 LOAP, les autorités de poursuite pénale de la Confédération sont la police et le MPC. L'art. 4 LOAP qualifie d'autorités de police (a) la Police judiciaire fédérale, (b) d'autres unités de l'Office fédéral de la police, lorsque le droit fédéral leur attribue des tâches en matière de poursuite pénale, (c) d'autres autorités fédérales, lorsque le droit fédéral leur attribue des tâches en matière de poursuite pénale et (d) les forces de police cantonales, lorsqu'elles accomplissent des tâches en matière de poursuite pénale en collaboration avec les autorités pénales de la Confédération. Divers offices fédéraux sont compétents en matière de poursuite d'infractions pénales (et aussi de crimes qui constituent une infraction préalable au blanchiment d'argent) dans le domaine du droit pénal administratif.

Le cercle des autorités auxquelles le MROS peut dénoncer des cas en vertu de l'art. 23 LBA s'étend donc au-delà des ministères publics cantonaux et du MPC. Le MROS se réserve donc le droit de transmettre à l'avenir des dénonciations également à la police ou aux autorités pénales administratives. Il consultera toutefois les autorités concernées au préalable. Celles-ci doivent noter qu'une dénonciation entraîne le blocage des valeurs patrimoniales. Si l'autorité souhaite maintenir le blocage des avoirs, elle doit rendre une décision dans un délai de cinq jours ouvrables (art. 10, al. 2 LBA).

¹⁰⁴ RS 312.0

¹⁰⁵ RS 173.71

6 Coopération internationale dans la lutte contre le blanchiment d'argent

6.1 Groupe Egmont

Le Groupe Egmont¹⁰⁶, un réseau mondial de CRF, a mené plusieurs activités importantes en 2024 dans le but de renforcer la lutte internationale contre le blanchiment d'argent et le financement du terrorisme.

Fin janvier 2024, plus de 400 représentants des CRF ainsi que des partenaires internationaux et des observateurs¹⁰⁷ ont participé à la 24e rencontre annuelle des groupes de travail et régionaux, qui s'est déroulée à St. Julian's, à Malte. La rencontre a porté sur la mise en œuvre de la stratégie 2022-2027 et l'identification de possibilités de soutien dans les domaines de la formation continue et de l'infrastructure technique des CRF. Les nouvelles technologies utilisées par les criminels et l'amélioration de l'échange d'informations entre les CRF ont également fait l'objet de discussions¹⁰⁸.

Organisée par la CRF française (Tracfin), la 30e réunion plénière annuelle du Groupe Egmont s'est tenue du 2 au 7 juin 2024 à Paris et a accueilli près de 400 représentants des CRF ainsi que des observateurs. Des invités d'honneur, dont le ministre français de l'Économie Bruno Le Maire et l'ancien président du GAFI T. Raja Kumar, de Singapour, ont ouvert les discussions. Le plénum a notamment abordé la thématique relative à la prochaine génération de CRF. La technologie et les ressources en personnel ne sont pas les seuls défis auxquels font face les CRF (cf. ch. 2.4) : le fait que les réseaux criminels accroissent et améliorent leur collaboration, aient recours à de nouvelles technologies et soient généralement mieux équipés que plusieurs CRF concernant les ressources techniques et informatiques représente un enjeu grandissant pour le Groupe Egmont¹⁰⁹.

Afin de renforcer la coopération internationale, le MROS s'engagera encore plus intensément dans son travail au sein du Groupe Egmont au cours des

deux prochaines années. En effet, à l'occasion de la réunion plénière qui s'est tenue à Paris, la cheffe suppléante du MROS et cheffe du Domaine Affaires internationales a été élue Représentante de la région Europe II pour un mandat de deux ans. En plus du MROS, les membres de cette région comprennent notamment le Royaume-Uni, Monaco, Guernesey, Jersey, Gibraltar, l'Île de Man, Israël, la Géorgie et l'Ukraine.

6.2 GAFI

6.0.1 Généralités

Le GAFI¹¹⁰ a franchi plusieurs étapes importantes en 2024 dans le but de renforcer la lutte internationale contre le blanchiment d'argent ainsi que le financement du terrorisme et de la prolifération.

En mars 2024, le GAFI a ainsi publié ses lignes directrices fondées sur les risques pour mettre en œuvre la recommandation 25 (transparence et bénéficiaires effectifs des constructions juridiques)¹¹¹. Les criminels utilisent frauduleusement des personnes morales, des trusts et d'autres constructions juridiques partout dans le monde pour dissimuler des valeurs patrimoniales à des fins de blanchiment d'argent, de financement du terrorisme, de corruption ou de contournement de sanctions. Les lignes directrices aident les États et le secteur privé à appliquer les exigences en matière de transparence aux conventions juridiques. Elles fournissent des indications pratiques permettant de comprendre et d'évaluer les risques liés aux constructions juridiques et aux trusts. Elles servent en outre à mieux identifier les criminels qui tentent de dissimuler leurs activités au moyen de sociétés écrans ou d'autres structures complexes.

La Suisse a conscience des risques liés aux valeurs patrimoniales criminelles dissimulées par le biais de structures juridiques. Par conséquent, le Conseil fédéral a adopté un message sur un projet

¹⁰⁶ Cf. [Rapport annuel 2023 du MROS](#), ch. 7.1.

¹⁰⁷ Les observateurs ne sont pas des CRF. Il s'agit d'institutions qui ont toutefois la possibilité de participer aux réunions du Groupe Egmont, telles qu'Europol, le GAFI ou l'Organisation mondiale des douanes.

¹⁰⁸ Groupe Egmont, [2024 Egmont Group Working and Regional Group Meetings \(St. Julian's, Malta\)](#) (en anglais), consulté le 31 janvier 2025.

¹⁰⁹ Groupe Egmont, [France's Financial Intelligence Unit \(Tracfin\) Hosts 400 EG Representatives from Around the Globe](#) (en anglais), consulté le 31 janvier 2025.

¹¹⁰ Pour davantage d'informations sur la structure et les tâches de l'organisation, cf. [Rapport annuel 2023 du MROS](#), ch. 7.2.

¹¹¹ GAFI, [Lignes directrices sur la transparence et les bénéficiaires effectifs des constructions juridiques](#)

de loi visant à renforcer la lutte contre le blanchiment d'argent et l'a transmis au Parlement en mai 2024. Ce projet vise à introduire un registre fédéral (registre de transparence) auquel les sociétés et les autres personnes morales devront annoncer l'identité de leurs ayants droit économiques. Grâce à ce registre, les autorités de poursuite pénale pourront notamment déterminer plus rapidement et avec une plus grande fiabilité qui est derrière une structure juridique. On empêchera ainsi que des personnes morales et des trusts soient utilisés en Suisse à des fins de blanchiment d'argent ou de dissimulation d'actifs¹¹².

En 2024, le GAFI a ajouté l'Algérie, l'Angola, la Côte d'Ivoire et le Liban à sa liste des juridictions faisant l'objet d'une surveillance accrue, alors qu'il en a retiré le Sénégal¹¹³. Il publie cette « liste grise » trois fois par année. Elle contient les pays et les juridictions qui présentent des défaillances dans la lutte contre le blanchiment d'argent et le financement du terrorisme. Ces pays coopèrent toutefois avec le GAFI pour remédier aux déficiences stratégiques de leur régime¹¹⁴.

Enfin, Elisa de Anda Madrazo, du Mexique, a été élue nouvelle présidente du GAFI pour une période de deux ans, du 1^{er} juillet 2024 au 30 juin 2026. Les priorités de la nouvelle présidence sont notamment la mise en œuvre de l'approche fondée sur les risques, le renforcement du réseau mondial, la mise en œuvre des normes du GAFI et la promotion de l'inclusion financière¹¹⁵.

6.0.2 Évaluations mutuelles

En octobre 2024, le GAFI a bouclé le quatrième cycle des évaluations mutuelles. Cet examen complet effectué par les pairs a permis d'analyser les mesures prises par plus de 200 États membres en matière de lutte contre la criminalité financière, le financement du terrorisme et la prolifération. Les rapports d'évaluation mutuelle examinent les progrès réalisés par un pays, mais soulèvent également ses lacunes. Le GAFI a tiré son bilan du quatrième cycle d'évaluation et a adopté des modifications pour

le cinquième cycle, qui concernent notamment la méthodologie et la procédure des évaluations mutuelles.

Le prochain cycle d'évaluation se concentrera encore davantage sur l'efficacité des dispositifs de lutte dans le but de veiller à ce que les pays appliquent bel et bien avec efficacité les lois, les prescriptions et les directives dont ils disposent. L'attention sera également davantage portée sur les principaux risques de chaque pays et le contexte dans lequel ils s'inscrivent. Ainsi, le GAFI s'assurera que les pays et les examinateurs se concentreront sur les domaines dans lesquels les risques sont les plus élevés, ceux présentant des risques moindres pouvant plus facilement faire l'objet d'enquêtes et de condamnations. À l'avenir, les recommandations tirées des rapports sur l'évaluation mutuelle seront davantage axées sur les résultats et se concentreront sur des calendriers et des mesures spécifiques en matière de lutte contre le blanchiment d'argent ainsi que le financement du terrorisme et d'armes de destruction massive. Le prochain cycle d'évaluation durera six ans, ce qui est nettement plus court que les cycles précédents et implique un engagement plus intense.

Les travaux préparatoires de la Suisse et donc du MROS ont commencé en vue du lancement du cinquième cycle d'évaluation. Le SFI dirige la coordination. Ces travaux préparatoires ne se limitent pas qu'aux autorités, mais concernent aussi le secteur privé, notamment les IF. Ces derniers jouent un rôle central dans l'évaluation car ils sont la « première ligne de défense » lorsqu'il est question de lutte contre le blanchiment d'argent et le financement du terrorisme.

À l'avenir, la Suisse mettra également à disposition des examinateurs qui évalueront d'autres pays. Elle veillera à leur formation dans le cadre des *Joint Assessor Trainings* pour qu'ils puissent remplir au mieux leur tâche exigeante. Ces formations, auxquelles les représentants des autorités des États

¹¹² Communiqué de presse du Conseil fédéral du 22 mai 2024 : [Le Conseil fédéral adopte le message sur le projet de loi visant à renforcer la lutte contre le blanchiment d'argent](#)

¹¹³ Publication du GAFI, [Résultats de la plénière du GAFI, 23-25 octobre 2024](#), 25 octobre 2024

¹¹⁴ Publication du GAFI, [La « liste noire » et la « liste grise »](#), consulté le 31 janvier 2025

¹¹⁵ Publication du GAFI, [Priorités pour la GAFI sous la Présidence du Mexique \(2024-2026\)](#), consulté le 31 janvier 2025

membres peuvent participer, ont lieu plusieurs fois par année.

6.3 Taskforces

Le MROS s'engage activement depuis des années dans plusieurs taskforces opérationnelles et stratégiques. Il a rejoint le Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS)¹¹⁶ début 2022 et le Counter Terrorist Financing Taskforce – Israel (CTFTI)¹¹⁷ fin 2023. Les objectifs et les activités de ces taskforces ont déjà été mentionnés dans le rapport annuel 2023. Ces deux taskforces se sont réunies à plusieurs reprises en 2024. Le MROS a eu l'occasion de les accueillir une fois chacune.

6.4 Rencontres bilatérales

Le MROS s'engage aussi pour une coopération efficace et sans faille avec les CRF partenaires étrangers. Pour lui, connaître les limites existantes et la marge de manœuvre juridique lorsqu'il souhaite obtenir des informations pertinentes auprès des autorités partenaires est essentiel non seulement pour clarifier rapidement les faits, mais aussi pour rationaliser ses ressources en personnel. Les rencontres bilatérales servent à l'échange stratégique et visent à optimiser la coopération, notamment dans le domaine de la criminalité organisée et du financement du terrorisme. Les moyens techniques liés à l'échange de données et le flux d'informations en constante augmentation sont également des thèmes qui concernent toutes les CRF et ont donc fait l'objet de discussions approfondies.

En 2024, le MROS a participé à plusieurs rencontres bilatérales, notamment avec les CRF des pays suivants: France, (Tracfin), États-Unis (FinCEN), Italie (UIF), Moldavie, Monténégro, Autriche (A-FIU), Hongkong (JFIU), Luxembourg (CRF) et Allemagne.

Fin septembre, le MROS a organisé la rencontre du Quad Island Forum (nouveau: Quad Forum)¹¹⁸, qui a duré trois jours et a notamment porté sur l'importance de la collaboration entre les autorités et le secteur privé. Sur la base de sa rencontre avec le Quad Island Forum qui s'était tenue en 2022 à Londres, le MROS a présenté le Swiss FIPPP annoncé alors et mis en œuvre en 2024. Les enjeux techniques et les quantités croissantes de données ont également été abordés. De précieux échanges ont eu lieu avec le Forum économique mondial (WEF)¹¹⁹ et le Wolfsberg Group¹²⁰. Les CRF du Luxembourg et de Monaco (Autorité Monégasque de Sécurité Financière) étaient également conviées.

Au mois de mai, les Pays-Bas ont organisé la réunion des CRF germanophones. Là aussi, l'une des questions centrales était la gestion de l'augmentation exponentielle des volumes de données, qui contraste avec la croissance modérée des ressources humaines et techniques. Enfin, les CRF présentes ont discuté de la prochaine évaluation mutuelle du GAFI.

À l'occasion de la réunion plénière du Groupe Egmont en juillet à Paris, le MROS a signé un mémorandum d'entente avec les CRF des Émirats arabes unis et de la Colombie, le but étant de renforcer la coopération avec ces pays.

¹¹⁶ [Financial Crimes Enforcement Network \(FinCen\), Russia-Related Illicit Finance and Sanctions FIU Working Group \(RRIFS Task Force\) \(en anglais\)](#), consulté le 31 janvier 2025

¹¹⁷ [Financial Crimes Enforcement Network \(FinCen\), Counter Terrorist Financing Taskforce – Israel \(CTFTI Task Force\) \(en anglais\)](#), consulté le 31 janvier 2025

¹¹⁸ Le Quad Island Forum (nouveau: Quad Forum) of Financial Intelligence Units est un regroupement stratégique des CRF de Gibraltar, Guernesey, Île de Man et Jersey.

¹¹⁹ Site Internet du [Forum économique mondial](#), consulté le 31 janvier 2025

¹²⁰ Site Internet du [Wolfsberg Group](#), consulté le 31 janvier 2025

7 Organisation du MROS

Le MROS est rattaché sur le plan organisationnel au Domaine de direction Prévention de la criminalité et droit de fedpol. Il est totalement indépendant dans son activité principale opérationnelle, ce qui lui permet de remplir les exigences internationales.

Le MROS est subdivisé en six domaines chargés de tâches spécifiques. En 2024, il employait en moyenne 60 collaborateurs (51 équivalents temps plein).

L'organigramme représente l'organisation actuelle du MROS.

Planification et affaires politiques (PuP)

Le Domaine PuP fonctionne comme une discipline transversale classique et se concentre sur diverses thématiques. Il traite toutes les questions juridiques ainsi que les dossiers politiques jusqu'au niveau du Conseil fédéral (par ex. projets de loi, motions, postulats, etc.). De plus, il suit et traite des projets et des publications (notamment rapports annuels, NRA et typologies), s'occupe de la gestion des risques et fait office d'interlocuteur pour toutes les demandes internes et externes aux niveaux formel et matériel. Il apporte son soutien aux domaines opérationnels du MROS et assure l'unité de doctrine. Il entretient des échanges réguliers avec d'autres autorités et s'occupe des questions administratives du MROS.

Analyse primaire (PA)

Le Domaine PA est responsable de l'enregistrement et de la préparation de toutes les communications entrantes du point de vue formel, technique et matériel. Il est aussi chargé des corrections manuelles lorsque la qualité des données n'est pas satisfaisante. Par ailleurs, il prend en charge le tri des cas, les transmet à un des domaines en aval sur la base d'une évaluation globale ou traite et transmet les communications directement aux autorités de poursuite pénale. Il est aussi compétent pour l'entraide administrative nationale au sens de l'art. 29 LBA.

Analyse opérationnelle Cantons (OAK)

Le Domaine OAK analyse les communications de soupçons entrantes qui relèvent en majorité de la compétence des autorités de poursuite pénale cantonales et lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées aux autorités de poursuite pénale compétentes, soit en général celles des cantons. Les informations peuvent aussi être partagées avec d'autres autorités nationales ou des CRF étrangères dans le cadre d'un échange d'informations. Les cas concernent notamment les infractions contre le patrimoine (principalement escroquerie, abus de confiance et gestion déloyale), la traite d'êtres humains et les faux dans les titres.

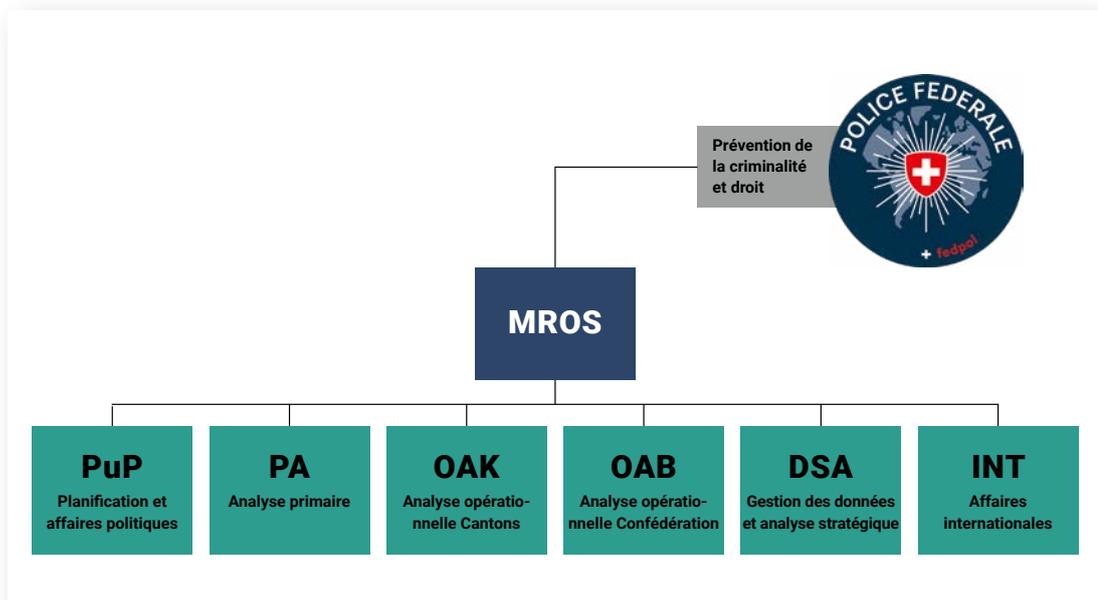


Fig. 14: Organigramme du MROS

Analyse opérationnelle Confédération (OAB)

Le Domaine OAB analyse les communications de soupçons entrantes qui relèvent a priori du MPC et lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées aux autorités de poursuite pénale compétentes, soit en général le MPC ou celles des cantons. Les informations peuvent aussi être partagées avec d'autres autorités nationales ou des CRF étrangères dans le cadre d'un échange d'informations. Les cas concernent notamment le blanchiment d'argent international (principalement corruption d'agents publics étrangers), la criminalité organisée, le terrorisme, les délits boursiers, l'extrémisme de droite et de gauche ainsi que le contournement de sanctions (infractions graves à la loi sur les embargos).

Gestion des données et analyse stratégique (DSA)

Le Domaine DSA est responsable de la sécurité d'exploitation et du développement technique du système d'information goAML. Dans ce cadre, il apporte un soutien technique aux IF, en particulier pour la programmation de leurs interfaces. Il est en outre chargé de développer les moyens techniques du traitement des données en lien avec des communications de soupçons. Il réalise les analyses stratégiques du MROS et exploite les données les plus diverses en rapport avec la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent et le financement du terrorisme, afin d'identifier les risques, les tendances et les méthodes propres au blanchiment d'argent.

Affaires internationales (INT)

Le Domaine INT se charge de l'ensemble des échanges (d'informations) avec les CRF étrangères, de l'adhésion à la Convention des Nations unies contre la corruption (CNUCC) ainsi que de la participation aux organes internationaux comme le Groupe Egmont, le GAFI et l'EFIPPP.

