



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 2025



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 2025

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	7
2	Développements stratégiques importants	8
2.1	Évaluation mutuelle du GAFI – aperçu	8
2.1.1	Situation	8
2.2	Le MROS en comparaison avec les CRF étrangères	10
2.3	Projets et outils informatiques	11
2.4	Rapports de typologie et typologies négatives	12
2.5	Partenariat public-privé (PPP)	12
2.5.1	Swiss FIPPP	12
2.5.2	EFIPPP	13
2.6	Évaluation nationale des risques (NRA)	14
2.7	Projets et événements	15
2.7.1	Global FIU Leadership Conference	15
2.7.2	3 ^e Crypto-Symposium du MROS	15
2.7.3	Underground banking roundtable	16
2.7.4	Rencontre sur les bonnes pratiques	16
3	Statistique annuelle du MROS	17
3.1	Constatations générales 2025	17
3.2	Communications de soupçons	18
3.3	Communications de soupçons par secteur d'activité des intermédiaires financiers	18
3.4	Bases légales des communications	20
3.5	Infractions préalables	20
3.6	Éléments à l'origine des soupçons	21
3.7	Dénonciations aux autorités de poursuite pénale	22
3.8	Retour d'information des autorités pénales	24
3.9	Financement du terrorisme	25
3.10	Criminalité organisée	25
3.11	Communications de soupçons en rapport avec les monnaies virtuelles	26
3.12	Remise d'informations en vertu de l'art. 11a LBA	27
3.13	Annonces de rupture de la relation d'affaires en vertu de l'art. 9b LBA	28
3.14	Échange d'informations avec les CRF étrangères	28
3.15	Échange d'informations avec les autorités suisses	29
4	Tendances	30
4.1	Escroquerie par piratage de la messagerie en entreprise	30
4.2	Flottes fantômes	31
4.3	Mafia italienne	33
5	Pratique du MROS	35
5.1	Changement de pratique: annonces de rupture selon la règle de minimis	35
5.1.1	Éléments clés de cette nouvelle pratique	35
5.1.2	Limites juridiques et pratiques de l'annonce de rupture préalable	35
5.2	Normes en matière de données	36
5.2.1	Normes en matière de données pour les communications de soupçons	36
5.2.2	Nouveauté législative: l'art. 23, al. 7, LBA	36
5.2.3	Mise en œuvre technique: procédés et perspective	36
5.2.4	XML Data Quality Report	36

6	Coopération internationale dans la lutte contre le blanchiment d'argent	38
6.1	Groupe Egmont	38
6.2	Groupe d'action financière (GAFI)	38
6.3	Taskforces	39
6.4	Rencontres bilatérales	39
7	Organisation du MROS	40

1 Avant-propos

L'année 2025 a été marquée par une nouvelle croissance significative du volume de communications et de données. Pendant l'année sous revue, le Bureau de communication en matière de blanchiment d'argent (MROS) a reçu au total 21 087 communications de soupçons, ce qui équivaut à une augmentation de 39,3% par rapport à l'année précédente et représente un nouveau record. Le MROS a reçu en moyenne 82 communications de soupçons par jour ouvrable. Depuis l'introduction du système d'information goAML en 2020, le volume des données entrantes a plus que quadruplé. La plupart des communications continue de provenir du secteur bancaire (91,3%). Parallèlement à cette hausse des communications entrantes, l'activité opérationnelle du MROS a également augmenté : 1375 cas ont été transmis aux autorités de poursuite pénale dans le cadre d'une dénonciation (+31,5% par rapport à 2024). En outre, l'utilisation d'instruments d'analyse approfondie s'est intensifiée, notamment dans le cadre de demandes d'informations en vertu de l'art. 11a de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA; RS 955.0) et d'un échange d'informations national et international toujours plus important. La forte augmentation du volume de données a accru les défis qualitatifs auxquels le MROS est confronté et par conséquent aussi les exigences en matière d'efficacité, d'établissement des priorités et de qualité des données.

Dans ce contexte, l'activité du MROS est restée résolument fondée sur l'analyse des risques et des renseignements. Le MROS a continué de mettre l'accent sur les affaires en lien avec la grande criminalité, notamment le crime organisé, le financement du terrorisme, les affaires complexes de fraude, la corruption, la traite d'êtres humains et le contournement de sanctions. L'étroite collaboration avec les autorités nationales de poursuite pénale, les autorités de surveillance et d'autres autorités compétentes, mais aussi avec les partenaires internationaux, est une condition essentielle à l'efficacité du dispositif suisse de lutte contre le blanchiment d'argent.

Un élément qui a revêtu une importance stratégique particulière pendant l'année sous revue était la préparation à la cinquième évaluation de la Suisse par le Groupe d'action financière (GAFI), qui aura lieu à partir de 2026. Le cycle d'évaluation actuel du GAFI

met l'accent sur l'efficacité du système et sa mise en œuvre pratique. Le MROS joue ici un rôle clé : en raison de son mandat légal et de sa fonction charnière entre marchés financiers et poursuite pénale, ses activités influencent l'évaluation de nombreux critères d'examen.

Au niveau international, le MROS a renforcé sa coopération avec les cellules de renseignement financier (CRF) étrangères et sa participation à divers organes multilatéraux et formes de coopération. L'échange transfrontalier d'informations a continué de gagner en importance, en particulier dans le contexte de l'augmentation d'affaires avec des ramifications internationales et des flux financiers complexes. La qualité, la rapidité et la fiabilité de cet échange sont déterminantes pour saisir au plus vite des valeurs patrimoniales et soutenir efficacement les enquêtes en cours.

Un autre objectif prioritaire était de développer davantage les bases techniques et organisationnelles du MROS. Plusieurs projets informatiques achevés ou en cours visaient à standardiser des processus, à accroître l'efficacité du traitement des cas et à faire en sorte que les données disponibles soient plus faciles à utiliser pour les analyses fondées sur les risques. Parallèlement, le fait de garantir une qualité élevée des données et des communications est resté une condition essentielle pour l'efficacité du travail d'analyse. Les initiatives entreprises dans ce sens concernent aussi bien les processus internes du MROS que l'interface avec les acteurs soumis à l'obligation de communiquer.

Le rapport annuel 2025 s'adresse aux autorités, aux intermédiaires financiers, aux décideurs politiques et au public spécialisé intéressé. Il vise à fournir une base factuelle permettant d'analyser les évolutions présentées ainsi que de contribuer au débat sur la structure et l'efficacité du dispositif suisse de lutte contre le blanchiment d'argent et le financement du terrorisme.

2 Développements stratégiques importants

2.1 Évaluation mutuelle du GAFI – aperçu

2.1.1 Situation

Entre fin 2026 et janvier 2028, la Suisse fera pour la cinquième fois l'objet d'une évaluation du GAFI¹ dans le cadre de son processus d'évaluation mutuelle.

Le GAFI, dont le siège se trouve à Paris, est l'organisme international chargé de fixer des normes visant à combattre et à prévenir le blanchiment d'argent ainsi que le financement du terrorisme et de la prolifération. Dans ses 40 recommandations², il définit des exigences et des critères uniformes destinés à l'ensemble du secteur financier ainsi qu'à d'autres personnes et groupes professionnels concernés. Leur mise en œuvre est vérifiée dans le cadre d'évaluations mutuelles périodiques, au cours desquelles les États membres du GAFI s'évaluent réciproquement. Les résultats sont consignés dans un rapport d'évaluation mutuelle (*Mutual Evaluation Report*, ou MER) et évalués au moyen d'une notation (*rating*). Le rapport est adopté par la Plénière du GAFI, qui peut ordonner des mesures de suivi en fonction de la notation obtenue.

Le GAFI n'est pas une organisation internationale au sens du droit international public, mais un organisme politique intergouvernemental. Ses recommandations n'ont donc pas d'effet légalement contraignant pour ses États membres. Elles n'en revêtent pas moins une importance considérable dans les faits : tout État qui ne les respecte pas est publiquement dénoncé par le GAFI. Trois fois par an, ce dernier publie des listes³ des États dont les mesures de lutte contre le blanchiment d'argent et le financement du terrorisme présentent des lacunes stratégiques. À cette fin, il établit une distinction entre deux types d'États. Sur la « liste noire », il répertorie les juridictions qui présentent de graves lacunes stratégiques dans la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération, et qui entravent, voire empêchent, les efforts internationaux dans ce domaine. La « liste grise » répertorie quant à elle les juridictions qui présentent des déficiences stratégiques dans leurs régimes de lutte contre le blan-

chiment d'argent, le financement du terrorisme et le financement de la prolifération, mais qui se sont engagées, en collaboration avec le GAFI, à y remédier dans des délais convenus et qui font donc l'objet d'une surveillance renforcée.

L'inscription d'un pays sur l'une de ces listes entraîne des conséquences réglementaires pour les autres États membres, notamment l'obligation de renforcer leurs mesures de réduction des risques. Les banques et les investisseurs sont tenus de classer la place financière concernée comme présentant un risque élevé, déclenchant ainsi une réaction en chaîne qui nuit à la réputation et à l'attractivité de cette dernière. Pour le pays concerné, cela se traduit par des obligations de diligence accrues, des délais de traitement plus longs lors des opérations de paiement et la restriction ou la suppression de relations avec des banques de correspondance. Les activités dans le domaine du financement du commerce et les relations de *clearing* en dollars américains sont régulièrement touchées par cette mesure. Des études empiriques ont montré qu'un tel statut peut s'accompagner d'un recul significatif de l'afflux de capitaux internationaux. Les secteurs exposés doivent en outre souvent envisager de délocaliser ou de transférer leurs activités à l'étranger afin de rester compétitifs. Un mauvais résultat lors de l'évaluation peut donc entraîner des conséquences économiques douloureuses.

La Suisse a été évaluée pour la dernière fois il y a dix ans. Le 7 décembre 2016, le GAFI a publié son quatrième rapport d'évaluation mutuelle sur la Suisse⁴. Il a alors constaté des lacunes dans la mise en œuvre de certaines recommandations dans neuf domaines. La Suisse a donc dû se soumettre à un suivi renforcé, qui s'est achevé à l'automne 2023. Le GAFI a salué les progrès réalisés par la Suisse, notamment par sa révision de la LBA, mise en œuvre en mars 2021. La Suisse a largement remédié aux problèmes signalés concernant six recommandations, notamment celle relative aux obligations de diligence des intermédiaires financiers envers leurs clients.

¹ [Groupe d'action financière \(GAFI\)](#)

² [Recommandations du GAFI](#)

³ [Listes du GAFI](#)

⁴ [Rapport d'évaluation mutuelle de la Suisse, décembre 2016](#)

Lors du cinquième cycle d'évaluation à venir, l'accent sera davantage mis sur l'efficacité du dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme et de la prolifération. Outre la transposition formelle des normes internationales dans le droit national, l'évaluation examinera de plus près la manière dont celles-ci sont appliquées dans la pratique. Sont considérées comme des preuves particulièrement solides d'une part les statistiques (par ex. nombre de communications de soupçons, d'analyses, de procédures pénales, de condamnations, de mesures prises, d'informations échangées au niveau national et international, etc.) et d'autre part les études de cas, qui permettent de présenter de manière compréhensible tant la collaboration entre les autorités et le secteur privé que de mettre en évidence les réussites.

L'évaluation débutera fin 2026 et se déroulera en deux parties. Dans un premier temps, une équipe composée de six à huit experts d'autres États membres procèdera à une analyse des bases légales et de la transposition des 40 recommandations du GAFI dans le droit suisse. Cette phase correspondra pour l'essentiel à une révision des documents. La deuxième partie consiste à examiner l'efficacité du dispositif de lutte contre le blanchiment d'argent. Dans ce cadre, une visite sur place (*On-site-visit*), soit une phase d'entretiens de trois semaines prévue pour le début de l'été 2027, revêt une importance capitale: lors de cette visite, différentes autorités, mais aussi des représentants du secteur financier, seront entendus sur le fonctionnement et l'efficacité du dispositif de lutte contre le blanchiment d'argent. À l'issue de l'évaluation, un avant-projet sera rédigé, puis consolidé sur la base de plusieurs prises de position, avant d'être négocié et adopté par les États membres lors de la réunion plénière de février 2028. Les rapports publiés jusqu'à présent dans le cadre du cinquième cycle d'évaluation⁵ révèlent que le GAFI adopte une approche plus stricte dans l'évaluation des différents aspects examinés.

L'évaluation d'efficacité comprend au total 11 chapitres (*immediate outcomes*, ou IO). Chaque IO reçoit une note selon les niveaux suivants: niveau d'efficacité élevé, niveau d'efficacité significatif,

niveau d'efficacité modéré et niveau d'efficacité faible. Les deux derniers niveaux sont considérés comme insuffisants.

Résultats immédiats du GAFI	
IO.1	Risques, politiques et coordination
IO.2	Coopération internationale
IO.3	Surveillance des instituts financiers (IF) et des prestataires de services d'actifs virtuels (PSAN)
IO.4	Surveillance des entreprises et professions non financières désignées (EPNFD)
IO.5	Personnes morales et trusts
IO.6	Renseignement financier
IO.7	Enquêtes et poursuites pénales en matière de blanchiment d'argent
IO.8	Confiscation / recouvrement d'avoirs
IO.9	Financement du terrorisme: enquêtes et poursuites pénales
IO.10	Financement du terrorisme: mesures préventives et sanctions
IO.11	Financement de la prolifération

Le MROS assume une fonction centrale dans l'évaluation du GAFI. Avec l'IO 6, il dispose de sa propre catégorie d'évaluation. Sur la base de son mandat légal (renseignement financier, coopération et prévention) et de son rôle charnière entre les marchés financiers et les autorités de poursuite pénale, il influence cependant aussi, par ses activités, de nombreux autres IO de manière plus ou moins directe. Il est donc essentiel que le MROS obtienne de bons résultats afin que le résultat global soit lui aussi favorable. Dans le cadre de l'évaluation du GAFI, toutes les autorités compétentes au niveau national dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme sont associées au processus d'évaluation: il s'agit des autorités de poursuite pénale de la Confédération et des cantons, des autorités de surveillance, du MROS ainsi que des autorités douanières et fiscales. Le Secrétariat d'État aux questions financières internationales (SFI) assure la coordination générale et la direction pour la Suisse. En vue de l'évaluation de la Suisse par le GAFI, le MROS a réalisé en interne une analyse des écarts (analyse GAP). L'objectif était d'identifier d'éventuelles lacunes structurelles ou opérationnelles, en tenant compte des conclusions de l'évaluation du GAFI de 2016 ainsi que de

⁵ Les évaluations réalisées jusqu'à présent dans le cadre du 5^e cycle portaient sur la Malaisie, la Belgique, Singapour, l'Italie et l'Autriche.

la liste de critères d'évaluation actuellement en vigueur. Les résultats de cette analyse sont pris en compte dans la préparation de l'évaluation.

2.2 Le MROS en comparaison avec les CRF étrangères

Compte tenu des défis opérationnels et financiers à venir, le MROS a mené en décembre 2024 et janvier 2025 un sondage auprès de six CRF étrangères comparables à celle de la Suisse sur le plan de la taille et du mandat⁶. Il portait notamment sur les défis actuels et futurs, l'efficacité des mesures visant à garantir la qualité des données, les instruments techniques utilisés et le personnel employé. L'objectif principal était de saisir les principales difficultés identifiées par les CRF et les approches organisationnelles et techniques qu'elles mettent en œuvre pour y faire face. Parallèlement, le MROS avait pour but d'approfondir les échanges internationaux existants et de mettre en place un partage d'expérience ciblé sur des questions spécifiques.

La grande majorité des CRF interrogées ont identifié comme principal défi la croissance continue du volume des communications et des données, alors que les ressources humaines et financières restaient limitées. Le développement et l'utilisation efficace de méthodes et d'outils d'analyse revêtent également une grande importance dans ce domaine. Parmi les mesures les plus efficaces pour relever ces défis, les CRF étrangères ont cité l'automatisation des étapes de travail, l'utilisation de méthodes de *data science* et l'adaptation ciblée des processus.

Face à l'augmentation du volume de données, il est d'autant plus important d'assurer la qualité des communications reçues. Les CRF ont mis en œuvre différentes mesures afin d'améliorer la qualité des données. Il s'agit d'une part d'approches systématiques de contrôle de la qualité des données ainsi que des processus techniques automatisés et manuels de nettoyage des données. D'autre part, les CRF misent sur la formation régulière des intermédiaires financiers auteurs de communications et des utilisateurs internes des bases de données. Par ailleurs, elles mettent continuellement à jour leurs

normes en matière de données et de documentation.

En ce qui concerne les solutions techniques utilisées, les CRF interrogées suivent toutes des approches hybrides largement comparables : *goAML* est l'application centrale, complétée par des applications développées en interne et par des fonctionnalités provenant des domaines du *data engineering* et de la *data science*, qui peuvent être combinées avec des composants *open source* et des solutions logicielles commerciales.

Toutes les CRF interrogées ont déclaré souhaiter promouvoir le développement ciblé de profils de postes spécialisés dans le traitement et l'analyse de données. Elles ont notamment cité des fonctions telles que *data scientist*, *software engineer*, *data analyst*, *knowledge management officer* ou *compliance officer* avec une orientation spécifique vers les données.

Les résultats du sondage confirment les conclusions que le MROS a également tiré de ses échanges internationaux continus. Ils montrent clairement que la croissance exponentielle des communications de soupçons ne peut être compensée uniquement par une augmentation des ressources humaines. Il s'agit plutôt de mettre en place une stratégie intégrée combinant l'automatisation des processus, l'investissement dans une infrastructure moderne de *data engineering* et de *data science*, ainsi que le développement ciblé de compétences supplémentaires au niveau du personnel en matière de traitement et d'analyse des données.

La comparaison internationale révèle qu'avec ses 57 postes à plein temps (ETP), le MROS dispose de ressources humaines relativement limitées par rapport à d'autres CRF compte tenu de l'importance de la place financière suisse et des risques particuliers liés à la gestion de fortune internationale. D'autres places financières internationales comparables à la Suisse, par exemple le Luxembourg (80 ETP), les Pays-Bas (110 ETP) ou Hong Kong (100 ETP) disposent de ressources en personnel nettement plus importantes au sein de leurs CRF respectives.

⁶ CRF Belgique, CRF Finlande, CRF Pays-Bas, CRF Luxembourg, CRF Danemark, CRF Hongkong

2.3 Projets et outils informatiques

Le MROS mène différents projets informatiques dans le but d'optimiser et de standardiser systématiquement ses processus opérationnels et de développer ses capacités d'analyse. Il met l'accent sur l'amélioration de l'efficacité dans la réception et le traitement des communications, ainsi que sur une meilleure utilisation des données disponibles pour les analyses fondées sur les risques. Plusieurs de ses projets ont pu être menés à bien en 2025.

Parmi les nouveautés introduites figure l'introduction d'un **accusé de réception automatisé** pour les communications de soupçons. En collaboration avec un fabricant du logiciel, une solution a été développée qui génère l'accusé de réception directement à partir du flux de travail en cours. Ainsi il n'est plus nécessaire de déclencher manuellement l'accusé de réception, comme c'était le cas auparavant. Cette adaptation contribue à réduire la charge administrative liée au traitement des cas.

Le MROS a encore gagné en efficacité grâce à l'introduction d'un nouveau **modèle de communication succincte** qui permet de transmettre de manière simplifiée et accélérée aux autorités de poursuite pénale les faits moins complexes. Des contenus qui devaient jusqu'à présent être créés en dehors de goAML, ce qui impliquait plusieurs changements de système, peuvent désormais être traités entièrement dans goAML. Cela permet également de réduire la charge administrative et de raccourcir le délai entre le dépôt d'une communication de soupçons par un intermédiaire financier et la transmission des informations pertinentes à l'autorité de poursuite pénale compétente.

Pour ce qui est du traitement des demandes d'entraide administrative, le MROS a mis en place un **processus de requête** qui permet aux autorités de poursuite pénale et à d'autres services administratifs autorisés d'effectuer des requêtes ciblées dans la base de données goAML. Dans le cadre des requêtes dites *hit/no hit* en vertu de l'art. 35, al. 2, LBA, les autorités requérantes peuvent apprendre si une personne, un compte, une adresse de portefeuille numérique ou une entreprise figure dans le système d'information goAML. Ces informations préliminaires servent à évaluer si une demande formelle d'entraide administrative est appropriée. L'objectif de ce processus est de réduire le nombre

de demandes formelles d'assistance administrative adressées au MROS ainsi que la charge administrative des deux côtés.

Outre les projets achevés, d'autres sont en cours de réalisation. Ceux-ci visent à optimiser les processus et à développer les capacités de traitement et d'analyse des données. Dans ce cadre, le MROS œuvre actuellement, en collaboration avec le Centre de services informatiques du Département fédéral de justice et police (CSI DFJP) et fedpol, au **développement de son infrastructure technique** afin de l'adapter aux exigences actuelles en matière de *data engineering* et aux approches modernes de la *data science*. Cette infrastructure élargie constitue une base pour la mise en œuvre d'autres projets, notamment le traitement largement automatisé de types de communications spécifiques, telles que les communications relatives aux *money mules* ou celles relatives aux ordonnances de production de pièces.

Un autre projet de développement central concerne la **mise en place d'un système de report (signalment) et de risk scoring (notation des risques)**. L'objectif de ce projet est de classer les éléments communiqués – en particulier les personnes, les comptes, les entreprises et les transactions – sur la base de critères définis en fonction du risque qu'ils représentent. Cela permettra de continuer à renforcer et à systématiser la priorisation des communications en fonction des risques. Une première composante de ce système global, appelé *report scoring*, est actuellement en phase de test. Le module plus complet de notation des risques est en cours de développement.

Les projets et développements informatiques décrits visent globalement à adapter les bases techniques et organisationnelles du MROS aux exigences d'un système de communication de plus en plus axé sur les données. L'automatisation systématique des processus, le développement ciblé de capacités d'analyse modernes et l'approche fondée sur les risques du traitement des communications permettent d'accroître l'efficacité, d'améliorer la qualité des analyses et d'utiliser plus efficacement les ressources disponibles. Le MROS contribue ainsi largement à renforcer la lutte contre le blanchiment d'argent et à soutenir efficacement les autorités de poursuite pénale et d'autres services compétents.

2.4 Rapports de typologie et typologies négatives

Garantir une qualité élevée des données et des communications est resté un objectif prioritaire du MROS en 2025. Si les lacunes formelles dans le système de communication ont davantage été mises en évidence ces dernières années, on constate aujourd'hui une baisse progressive de la qualité des communications de soupçons. Le MROS souligne depuis plusieurs années l'importance capitale de la qualité des données et des communications, comme il l'a fait récemment dans son rapport annuel 2024 (ch. 5.1) et auparavant dans ses rapports annuels 2023 (ch. 2.1 et 2.2) et 2022 (ch. 2.3.5).

Le MROS poursuit une approche multidimensionnelle dans son projet d'améliorer la qualité des communications: outre l'échange direct avec les intermédiaires financiers individuels, il mise sur des formats ciblés de sensibilisation et de transmission du savoir, notamment des formations, des rencontres spécialisées et des publications thématiques. Les **rapports de typologie** jouent un rôle central à cet égard: ces documents présentent des exemples anonymisés qui illustrent des cas typiques pouvant se produire dans un domaine donné, afin de montrer les meilleures pratiques et fournir des aides concrètes pour effectuer des clarifications. En septembre 2025, le MROS a publié son deuxième rapport de typologie, consacré au phénomène des *enablers*.

En complément à ces typologies des bonnes pratiques, le MROS a publié pour la première fois en août 2025 des **typologies négatives**. Il s'agit de présentations fortement simplifiées de situations sélectionnées, qui permettent d'illustrer les lacunes récurrentes dans les communications de soupçons. Tout comme les bonnes pratiques, les typologies négatives ne constituent ni une interprétation normative, ni une directive: elles servent exclusivement à sensibiliser les intermédiaires financiers

concernant les lacunes typiques des communications et à les inciter à examiner de manière plus approfondie l'arrière-plan des relations d'affaires ou transactions, les éventuelles infractions préalables ainsi que l'ensemble des faits pertinents en matière de blanchiment d'argent. Une communication de soupçons fondée, soigneusement vérifiée et documentée de manière compréhensible est une condition essentielle pour lutter efficacement contre le blanchiment d'argent et le financement du terrorisme. Elle est également indispensable pour assurer un usage approprié des instruments technologiques perfectionnés, en particulier les méthodes d'analyse basées sur les données et les logiciels d'analyse modernes. La responsabilité d'évaluer si un fait donné est soumis à l'obligation de communiquer conformément à l'art. 9 LBA incombe dans tous les cas à l'intermédiaire financier concerné et dépend de chaque situation individuelle.

2.5 Partenariat public-privé (PPP)

2.5.1 Swiss FIPPP

Le *Swiss Financial Intelligence Public Private Partnership* (Swiss FIPPP) est un partenariat stratégique entre le MROS et des établissements financiers du secteur privé suisse. Il a pour objectif l'échange structuré d'informations afin d'identifier, d'analyser et de catégoriser à un stade précoce les risques et les menaces dans le domaine du blanchiment d'argent et du financement du terrorisme.

Le Swiss FIPPP a démarré ses activités fin 2024. Son travail se concentre essentiellement sur l'analyse stratégique des méthodes, des tendances et des évolutions des phénomènes criminels liés au blanchiment d'argent et au financement du terrorisme. Sur cette base, il élabore des caractéristiques distinctives (indicateurs) ainsi que des descriptions de modes opératoires nouveaux ou en mutation (typologies) afin d'identifier plus rapidement les menaces potentielles. L'échange d'informations aide le



Fig. 1: Logo du Swiss FIPPP



Fig. 2: Logo de l'EFIPPP

secteur privé à identifier de manière plus ciblée les situations suspectes et sert de base aux autorités pour prendre des mesures préventives et engager des poursuites pénales.

Les activités du Swiss FIPPP sont coordonnées par un comité dont les membres sont élus par l'assemblée plénière. Le MROS se charge de l'organisation et de la communication. En 2025, trois séances plénières ont eu lieu, auxquelles tous les membres ont participé. En outre, des groupes de travail thématiques se sont réunis régulièrement. Il en existe actuellement deux: le groupe de travail *Regulatory and innovation* traite des questions techniques et liées aux processus, en particulier la qualité des données et l'amélioration des communications de soupçons. Le groupe de travail *Threats and typologies* s'est concentré en 2025 sur les phénomènes de la traite d'êtres humains et de l'escroquerie.

Le Swiss FIPPP publie régulièrement des informations adaptées au public sur ses activités et ses résultats. En décembre 2025, il a publié une newsletter sur le thème des escroqueries liées aux IBAN virtuels: ces derniers sont de plus en plus utilisés, décuplant ainsi les possibilités pour les criminels d'en faire un usage frauduleux⁷. La newsletter vise à sensibiliser les intermédiaires financiers à ce type d'escroquerie et à leur présenter des mesures pratiques pour faire face aux risques qu'elle comporte.

Le Swiss FIPPP est conçu comme un partenariat dynamique et évolutif. Il analyse en permanence les besoins des membres et l'évolution du marché financier en tenant compte des expériences internationales avec des modèles comparables de partenariats public-privé, dont certains prévoient déjà des formes de coopération approfondie, y compris opérationnelles.

2.5.2 EFIPPP

En 2025, le MROS a poursuivi son engagement au sein du *Europol Financial Intelligence Public Private Partnership* (EFIPPP). L'EFIPPP est une plateforme de coopération transnationale visant à favoriser les échanges structurés entre les CRF, les autorités de poursuite pénale, les autorités de surveillance et certains représentants du secteur privé. Il se concentre sur la prévention et la lutte contre les formes complexes de criminalité financière et économique.

Pendant l'année sous revue, le MROS a participé à plusieurs séances plénières de l'EFIPPP. Celles-ci portaient entre autres sur des thèmes prioritaires tels que « *Underground banking* » et « *Unmasking the financial footprints of synthetic drug trafficking* ». Le MROS a notamment contribué à ces discussions en partageant son expérience du système suisse de communication de soupçons ainsi que des enseignements tirés de l'analyse opérationnelle et stratégique de ces communications. Ces rencontres lui ont également permis d'échanger avec d'autres partenaires sur les approches existantes et les expériences acquises.

Au niveau stratégique, le MROS était également représenté au sein du *steering committee* de l'EFIPPP en 2025. À ce titre, il a contribué à définir le contenu de la plateforme, à fixer des priorités thématiques et à coordonner les activités des groupes de travail. Il a aussi participé au développement de la coopération entre les autorités publiques et les acteurs privés.

Le MROS participe activement aux groupes de travail consacrés à la traite d'êtres humains (*Trafficking in Human Beings*, THB), aux abus sexuels et à l'exploitation des enfants (*Child Sexual Abuse*

⁷ <https://www.fedpol.admin.ch/dam/en/sd-web/KBBXGI1w-FxY/fippp-newsletter-2025-12.pdf> (en anglais uniquement)

and Exploitation, CSAE), ainsi qu'aux facilitateurs professionnels (*Professional Enablers*). De plus, le MROS est co-président depuis 2025 du groupe de travail sur l'innovation.

Par son engagement continu au sein de l'EFIPPP, le MROS contribue à la mise en réseau internationale, à l'échange d'expériences et soutient le développement d'approches communes pour lutter contre le blanchiment d'argent, le financement du terrorisme ainsi que d'autres formes graves de criminalité économique et financière.

2.6 Évaluation nationale des risques (NRA)

L'évaluation des risques liés au blanchiment d'argent et au financement du terrorisme constitue un élément essentiel de la stratégie nationale de lutte contre la criminalité financière. C'est pourquoi la Suisse procède régulièrement à des évaluations nationales des risques (*National Risk Assessments*, NRA) et en publie les résultats. Outre deux rapports NRA intersectoriels publiés en 2015⁸ et 2021⁹, il a produit de nombreux rapports sectoriels ou thématiques¹⁰.

La coordination des analyses de risque nationales est dirigée par le groupe de coordination interdépartemental pour la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération (GCBF). Le GCBF est une plateforme de coordination permanente créée par le Conseil fédéral, chargée de coordonner la politique suisse dans les domaines mentionnés. Le MROS est membre du GCBF et assume, en tant que responsable du sous-groupe « Analyse des risques », un rôle de premier plan dans l'élaboration des rapports sur les risques.

En milieu d'année 2026, le GCBF publiera le rapport sectoriel sur les risques intitulé *National Risk Assessment: Juristische Personen und Rechtsvereinbarungen*, que le MROS a rédigé en collaboration avec des experts de différentes autorités administratives.

Les personnes morales, trusts et autres structures similaires jouent régulièrement un rôle central dans les affaires de blanchiment d'argent. Le rapport sectoriel confirme dans une large mesure les conclusions d'une autre analyse sectorielle publiée en 2017 concernant les personnes morales. Les personnes morales et les accords juridiques étrangers continuent de présenter des risques plus élevés que leurs équivalents suisses. La forme juridique exacte revêt ici une importance secondaire. Ce qui importe davantage, c'est de savoir si une personne morale exerce une activité opérationnelle effective. Les sociétés de domicile présentent un risque de fraude nettement plus élevé, en particulier lorsqu'il s'agit de sociétés écran. Les structures transfrontières complexes ou l'absence d'objectif économique augmentent considérablement le risque d'abus. Dans ce contexte, les avocats, notaires et fiduciaires jouent un rôle particulièrement important lorsqu'ils participent à la création ou à la structuration d'un tel montage.

Dans le même temps, la Suisse a considérablement renforcé le cadre réglementaire et comblé des lacunes juridiques: les actions au porteur ont été en principe supprimées; les sociétés commerciales suisses ont été obligées de tenir un registre des actions ou des parts; et des sanctions ont été introduites en rapport avec la tenue de ces registres ainsi que des obligations de vérification des intermédiaires financiers en matière d'informations sur les ayants droit économiques. Ces mesures visent en particulier à réduire les risques liés aux personnes morales suisses, notamment les sociétés anonymes.

Avec l'adoption de la loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques (LTPM) et la révision de la LBA en septembre 2025, la Suisse a encore renforcé son dispositif de lutte contre le blanchiment d'argent. Ces nouveautés visent à accroître la transparence des personnes morales suisses et étrangères ainsi qu'à permettre aux autorités compétentes d'accéder plus efficacement aux informations sur les ayants droit économiques. Parallèlement, certaines activités des conseillers et des avocats sont désor-

⁸ [Premier rapport national sur les risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), juin 2015

⁹ [Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme en Suisse](#), octobre 2021

¹⁰ [Publications du Bureau de communication en matière de blanchiment d'argent \(MROS\)](#)

mais réglées par la LBA. L'efficacité des mesures adoptées dans le cadre de la LTPM et de la LBA révisée devra être observée au cours des années à venir.

2.7 Projets et événements

En 2025, le MROS a organisé diverses rencontres spécialisées à l'échelon national et international. Ces formats permettent aux participants d'échanger dans un cadre confidentiel au sujet des développements actuels et des défis opérationnels, tout en renforçant la coopération transfrontière. Ils contribuent à l'identification précoce de nouveaux risques et à la mise en place de structures de prévention et d'enquête plus efficaces en matière de blanchiment d'argent – une plus-value qui, en fin de compte, renforce durablement l'ensemble du système de lutte contre le blanchiment d'argent, y compris dans le secteur financier.

2.7.1 Global FIU Leadership Conference

Du 14 au 15 octobre 2025, le MROS a accueilli la conférence mondiale des dirigeants de CRF (*Global FIU Leadership Conference*). Organisée en collaboration avec ECOFEL¹¹ et avec le soutien du Secrétariat d'État à l'économie (SECO), cette conférence a permis aux dirigeants des CRF d'échanger leurs points de vue, complétant ainsi les formats d'échange existants dans le cadre de la coopération internationale entre CRF.

Dans un environnement technologique et financier en pleine mutation, les CRF sont de plus en plus confrontées à des tâches d'analyse et de coordination complexes. Face aux développements internationaux, aux innovations technologiques et à l'augmentation du volume des communications, de nombreuses CRF se trouvent confrontées à des difficultés comparables.

La conférence a abordé des questions stratégiques liées à la lutte contre le blanchiment d'argent et le financement du terrorisme. Parmi les thèmes abordés figuraient notamment les développements dans le domaine des technologies de l'information et de l'intelligence artificielle, les questions organi-

sationnelles ainsi que les perspectives à moyen et long terme pour les CRF. Les échanges ont porté en particulier sur la meilleure manière de structurer les processus internes, sur l'utilisation des outils techniques et sur la coopération internationale.

Placée sous la devise *Back to the future*, cette conférence était une occasion de discuter des structures existantes et des évolutions possibles de l'architecture internationale en matière de renseignement financier.

2.7.2 3^e Crypto-Symposium du MROS

Le 3 novembre 2025, le MROS a tenu son troisième *Crypto-Symposium*. Quelque 280 représentants de différentes autorités, du secteur financier et d'organisations internationales y ont participé. Les intervenants ont abordé la question de l'efficacité au niveau de la gestion des risques liés aux cryptomonnaies dans le domaine du blanchiment d'argent et du financement du terrorisme.

Pour commencer, des experts du Forum économique mondial (*Cybercrime Atlas*) et d'Europol ont présenté une vue d'ensemble des approches de coopération internationale dans la lutte contre la cybercriminalité et la criminalité financière, en mettant l'accent sur les mécanismes de coopération transfrontaliers. Un représentant de l'école supérieure de police et d'administration publique de Rhénanie-du-Nord-Westphalie a expliqué les interdépendances techniques dans la lutte contre la criminalité financière, mentionnant notamment le recours à des outils d'analyse spécialisés et les questions liées à la transparence et au contrôle des systèmes techniques. Le MROS a présenté des typologies nationales et les évolutions récentes dans le domaine des cryptomonnaies. L'après-midi était consacré à des études de cas. La CRF du Kazakhstan a présenté le cas d'un système de Ponzi transnational. L'entreprise technologique étasunienne TRM Labs a quant à elle décrit des faits liés aux cryptomonnaies en rapport avec des violences sexuelles sur mineurs. Enfin, la CRF des Émirats arabes unis et l'Office fédéral de police criminelle autrichien ont présenté d'autres analyses pratiques.

¹¹ ECOFEL fait partie du Groupe Egmont et apporte son soutien aux membres de ce dernier, entre autres sous la forme de mesures ciblées visant à renforcer les capacités, telles que l'évolution des cadres dirigeants, des e-learning et des formations spécialisées.

La rencontre s'est achevée par un panel de discussion réunissant des représentants des secteurs public et privé. Les discussions ont porté sur des questions de coopération, d'échange d'informations et de défis opérationnels.

Le lendemain, les représentants d'autorités se sont par ailleurs réunis pour un échange interne consacré à des questions opérationnelles et techniques.

2.7.3 Underground banking roundtable

La deuxième table ronde sur les opérations bancaires clandestines (*Underground banking roundtable*) s'est tenue à Berne les 20 et 21 novembre 2025. Le terme d'*underground banking* désigne les systèmes financiers informels qui opèrent en dehors du secteur bancaire réglementé et qui permettent d'effectuer des transferts de fonds internationaux sans passer par des établissements agréés¹².

De tels systèmes existent depuis longtemps sous différentes formes et sont utilisés aussi bien à des fins légales qu'illégales. Les analyses et enquêtes actuelles portent en particulier sur les formes numériques de ce phénomène.

Près de 80 représentants des autorités de poursuite pénale et des CRF ont participé à la table ronde. Les contributions d'Interpol, d'Europol, du *Eastern and southern africa anti-money laundering Group* (ESAAMLG) et de l'Office des Nations Unies contre la drogue et le crime (ONUDC) ont présenté des typologies, des développements opérationnels et des études de cas. Les participants ont également discuté des défis pratiques et des approches possibles en matière d'enquête.

2.7.4 Rencontre sur les bonnes pratiques

À l'automne 2025, le MROS a organisé, en collaboration avec l'Association suisse des banquiers (ASB), un séminaire spécialisé intitulé « Bonnes pratiques en matière de communications de soupçons – le point de vue de MROS ».

Cette manifestation a offert aux participants une vue d'ensemble du mandat, de la fonction et du mode de fonctionnement du MROS, tout en décri-

vant l'évolution du dispositif législatif en matière de blanchiment d'argent. L'accent a été mis sur le mode de travail analytique du MROS et sur les informations pertinentes dont il a besoin pour ce faire. Il a notamment été thématiqué la nécessité de fournir des informations complètes et structurées dans les communications de soupçons. Le séminaire a également abordé l'importance des clarifications prévues à l'art. 6 LBA, étant donné que le MROS ne procède pas lui-même à des clarifications directes auprès des personnes faisant l'objet d'une communication. Des questions relatives à l'échange institutionnel et au cadre juridique en matière de protection des données ont également été évoquées. Ce séminaire a permis un échange spécialisé entre les intermédiaires financiers et les autorités dans le cadre des dispositions légales en vigueur.

¹² [Underground Banking](#)

3 Statistique annuelle du MROS

Le MROS génère des statistiques anonymisées afin d'analyser les informations relatives au blanchiment d'argent, aux infractions préalables au blanchiment d'argent, à la criminalité organisée et au financement du terrorisme au cours de l'exercice sous revue¹³. Ces statistiques comprennent notam-

ment les communications de soupçons transmises au MROS par les intermédiaires financiers, les demandes de renseignements d'autorités étrangères compétentes ainsi que les procédures faisant suite aux communications (cf. art. 23, al. 1, OBCBA¹⁴).

3.1 Constatations générales 2025

- Pendant l'année sous revue, le MROS a reçu un total de **21 087** communications de soupçons, soit en moyenne 82 par jour ouvrable. Par rapport à 2024 (15 141), ce nombre représente une augmentation de **39,3%**. Depuis l'introduction du système d'information goAML en janvier 2020, le volume de communications a presque quadruplé. Les communications proviennent pour **91,3%** d'intermédiaires financiers du **secteur bancaire** (moyenne 2016 – 2025: 90,1%).
- En 2025, le MROS a transmis **1375** cas aux **autorités de poursuite pénale**, ce qui représente une hausse de **31,5%** par rapport à l'année précédente. Un rapport d'analyse contenant les informations pertinentes est transmis aux autorités de poursuite pénale dans chaque cas. Une transmission peut se fonder sur plusieurs communications de soupçons et informations qui ne sont pas nécessairement parvenues au MROS au cours de la même année civile. Les informations peuvent provenir de différentes autorités suisses et étrangères.
- Dans le cadre de ses travaux d'analyse approfondis, le MROS a adressé pendant l'année sous revue **1096 demandes d'informations en vertu de l'art. 11a LBA** à des intermédiaires financiers auteurs de communications ou à des intermédiaires tiers, ce qui correspond à une **augmentation de 7,9%** par rapport à l'année précédente. Environ un cas sur cinq (20,1%) transmis aux autorités de poursuite pénale contenait des informations supplémentaires issues de demandes adressées par le MROS aux intermédiaires financiers.
- L'échange national d'informations entre le MROS et les autres autorités suisses a continué d'augmenter en 2025. Par rapport à 2024, le nombre d'**informations spontanées transmises par le MROS** à d'autres autorités suisses a augmenté de **36,9%**, atteignant le nombre de 490. De même, les autorités suisses ont adressé davantage d'informations spontanées au MROS (2025: **120**; **+13,2%** par rapport à l'année précédente) et davantage de requêtes d'informations (2025: **498**; **+11,4%** par rapport à l'année précédente).
- En ce qui concerne l'**échange d'informations international** avec les CRF étrangères, on a constaté en 2025 une évolution différente des autres années. Le MROS a reçu **660** requêtes d'informations de CRF étrangères, ce qui représente une baisse de **15,1%**. En revanche, il a reçu **932 informations spontanées**, soit une augmentation de **24,1%**. De son côté, le MROS a adressé 236 requêtes d'information à des CRF étrangères (-1,3% par rapport à l'année précédente) et 223 informations spontanées (+6,6% par rapport à l'année précédente).

¹³ Exercice sous revue: du 1^{er} janvier au 31 décembre de l'année concernée

¹⁴ Ordonnance sur le Bureau de communication en matière de blanchiment d'argent (OBCBA; RS 955.23)

3.2 Communications de soupçons

En 2025, le MROS a reçu 82 communications de soupçons en moyenne par jour ouvrable, ce qui équivaut à 21 087 communications au total transmises par des intermédiaires financiers ou des négociants. Cela représente une augmentation de 39,3% par rapport à l'année précédente. Ce nombre de communications reçues a presque quadruplé depuis que le système d'information goAML a été introduit en 2020 (cf. Fig. 3)¹⁵.

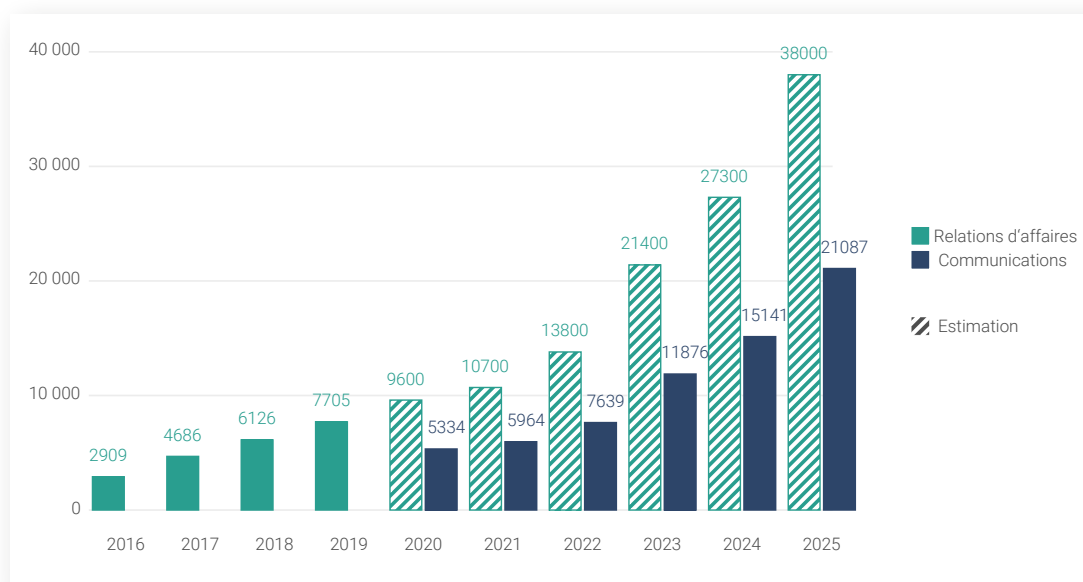
Comme le montre la Fig. 3, le nombre de relations d'affaires signalées chaque année a été multiplié par 13 depuis 2016 : alors que, cette année-là, 2909 relations d'affaires suspectes avaient été communiquées au MROS, on en dénombrait environ 38 000 en 2025. Cette évolution est notamment due à l'augmentation du nombre de communications engendrée par les adaptations législatives et les

progrès dans la numérisation, en particulier dans les domaines de la surveillance des transactions et des processus d'analyse internes des intermédiaires financiers (par ex. grâce à des outils plus performants)¹⁶.

3.3 Communications de soupçons par secteur d'activité des intermédiaires financiers

En 2025, 91,3% des communications de soupçons reçues par le MROS provenaient d'intermédiaires financiers du secteur bancaire. Le comportement de ces intermédiaires 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)¹⁷.

Fig. 3 : Nombre de relations d'affaires et de communications de soupçons signalées 2016 – 2025



¹⁵ 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. 3 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 21 087 communications de soupçons de 2025 correspondent à environ 38 000 relations d'affaires.

¹⁶ Cf. explications dans le [rapport annuel 2023 du MROS](#), ch. 2.1

¹⁷ L'intermédiaire financier procède lui-même au choix du secteur d'activité lors du processus d'enregistrement dans goAML. Ensuite, le MROS vérifie au moyen d'un contrôle de plausibilité si la classification est correcte. Ce contrôle se base sur les listes publiques de la FINMA ou sur les indications du site Internet d'un OAR, permettant de déterminer le secteur d'activité par déduction. Une classification trop approximative reste toutefois possible, en particulier dans des secteurs hétérogènes tels que la gestion de fortune.

Tabl. 1 : Communications de soupçons par secteur 2016 – 2025¹⁸

Secteur	2016 ^A	2017 ^A	2018 ^A	2019 ^A	2020 ^B	2021 ^B	2022 ^B	2023 ^B	2024 ^B	2025 ^B	2025 en chiffres absolus	Moyenne 2016–2025
Banques	86%	91%	88,8%	89,9%	89,5%	90%	91,6%	90,5%	92,3%	91,3%	19 246	90,1%
Prestataires de services de paiement	4,4%	3,1%	4,4%	4%	3,5%	2,5%	2%	2,8%	2,2%	2,6%	545	3,2%
Autres intermédiaires financiers	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2%	0,2%	2,1%	446	1,5%
PSAV / Fintech									1,5%	1,3%	276	1,4%
Émetteurs de cartes de crédit	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	1,6%	1,3%	275	1,3%
Maisons de jeu	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	0,3%	0,3%	68	0,5%
Gérants de fortune / Conseillers en placement	2,2%	1,9%	1%	0,9%	0,8%	1%	0,6%	0,8%	0,9%	0,3%	65	1%
Opérations de crédit, de leasing, d'affacturage et de financement à forfait	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	0,2%	0,2%	41	0,3%
Fiduciaires	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	0,2%	0,2%	36	0,6%
Maisons de titres	0,1%	0,3%	0,1%	0,3%	0%	0,2%	0,1%	0,2%	0,2%	0,1%	30	0,2%
Assurances	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	0,2%	0,1%	26	0,6%
Négociants en matières premières et métaux précieux	0,1%	0,2%	0%	0,3%	0,2%	0,5%	0,3%	0,3%	0,2%	0,1%	20	0,2%
Bureaux de change	0%	0%	0%	0%	0,1%	0,1%	0,3%	0,6%	0%	0%	4	0,1%
OAR	0%	0%	0%	0,1%	0%	0%	0%	0,1%	0%	0%	3	0%
Négoce de devises	0,1%	0%	0%	0,3%	0%	0%	0%	0%	0%	0%	2	0%
Avocats et notaires	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0%	0,1%	0%	0%	2	0,1%
Distributeurs de fonds de placement	0%	0,1%	0%	0%	0%	0%	0%	0%	0%	0%	1	0%
Autorités (FINMA/ CFMJ/ GESPA et les autorités intercantionales)	0%	0%	0%	0%	0%	0,1%	0%	0%	0%	0%	1	0%
Trustees	0%	0%	0%	0%	0,1%	0,1%	0%	0%	0%	0%		0%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	21 087	100,0%

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

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

Présentés depuis 2024 dans une catégorie distincte, les prestataires de services d'actifs virtuels (PSAV) et dans le domaine Fintech ont soumis 276 communications de soupçons au MROS (1,3%) au cours de l'exercice sous revue, ce qui correspond à une baisse de 0,2% par rapport à l'année précédente.

¹⁸ Les chiffres absolus pour les années 2016-2024 sont présentés dans les rapports annuels respectifs du MROS.

3.4 Bases légales des communications

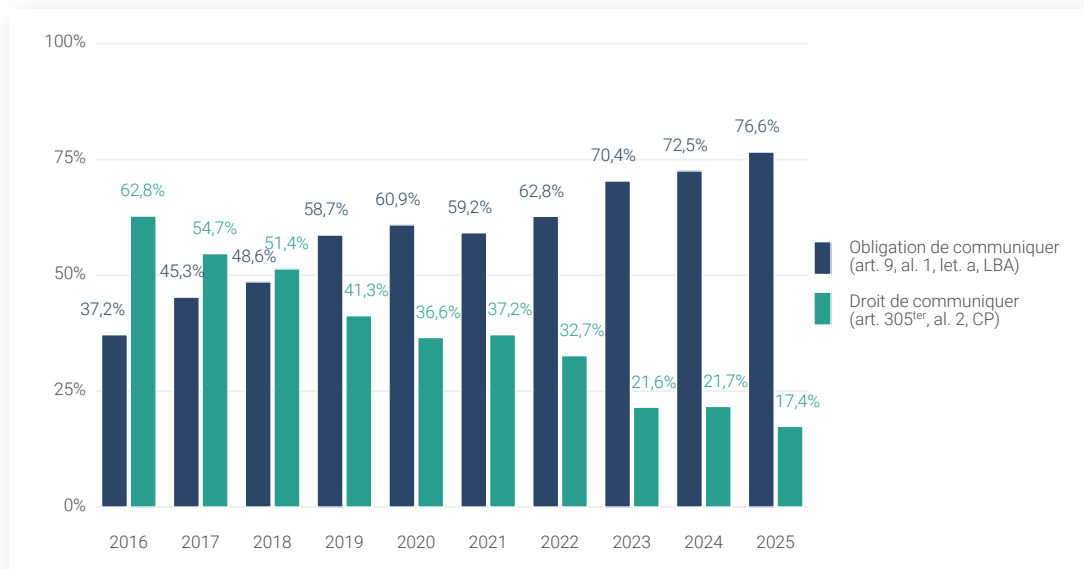
La base légale d'une communication de soupçons dépend du degré de suspicion. S'ils ont des soupçons fondés, les intermédiaires financiers ont l'obligation de les communiquer au MROS en vertu de l'art. 9, al. 1, let. a, LBA¹⁹. S'ils n'ont que de simples soupçons, ils peuvent s'appuyer sur le droit de communiquer prévu à l'art. 305^{ter}, al. 2, CP²⁰. En 2025, les communications transmises relevaient dans 76,6% des cas de l'obligation de communiquer (art. 9, al. 1, let. a, LBA; cf. fig. 4) et dans 17,4% des cas du droit de communiquer (art. 305^{ter}, al. 2, CP). Dans 5,7% des cas, les intermédiaires financiers 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. 4)²¹.

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). Cette tendance s'est poursuivie en 2025, où le recours à l'obligation de communiquer dans le cadre d'une relation d'affaires existante a augmenté de 4,1% par rapport à l'année précédente, tandis que le droit de communiquer a été nettement moins utilisé (-4,3%). Les communications des intermédiaires financiers en cas de rupture des négociations visant à établir une nouvelle relation d'affaires conformément à l'art. 9, al. 1, let. b, LBA sont restées stables (+0,1%).

3.5 Infractions préalables

Lors d'une communication, les intermédiaires financiers indiquent à chaque fois l'infraction préalable ou

Fig. 4: Communications relatives à des relations d'affaires existantes par base légale 2016 – 2025



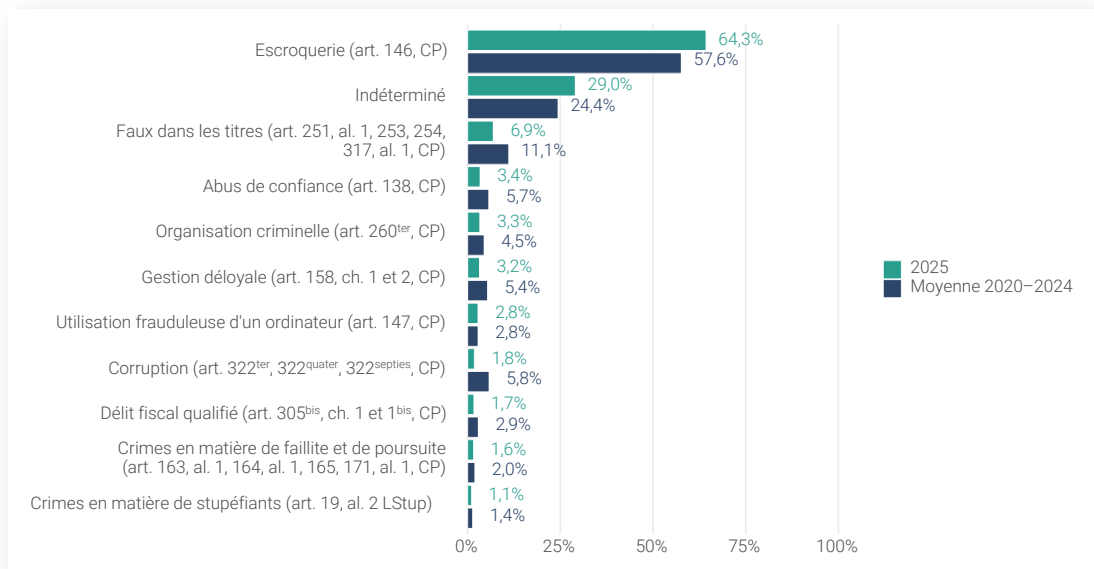
¹⁹ « L'intermédiaire financier informe immédiatement le Bureau de communication en matière de blanchiment d'argent au sens de l'art. 23 (bureau de communication) s'il sait ou présume, sur la base de soupçons fondés, que les valeurs patrimoniales impliquées dans la relation d'affaires ont un rapport avec une des infractions mentionnées aux art. 260^{ter} ou 305^{bis} CP, qu'elles proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305^{bis}, ch. 1^{bis}, CP, qu'elles sont soumises au pouvoir de disposition d'une organisation criminelle ou terroriste, ou qu'elles servent au financement du terrorisme (art. 260^{quinquies}, al. 1, CP) » (art. 9, al. 1, let. a, LBA).

²⁰ « 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^{bis} » (art. 305^{ter}, al. 2, CP).

²¹ « 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 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).

Fig. 5: Fréquence des infractions préalables présumées

2020 – 2025, fréquence, exprimée en % du nombre total de communications (plusieurs réponses possibles)



les infractions préalables qu'ils présument. En 2025, l'infraction préalable présumée la plus fréquemment citée était l'escroquerie. Seule ou en combinaison avec d'autres infractions, celle-ci concernait 64,3% des communications. Un taux qui la situe au-dessus de la moyenne des années ayant suivi l'introduction du système goAML (moyenne 2020-2024: 57,6%, cf. fig. 5)²². D'autres infractions préalables ont été beaucoup plus rarement nommées. Parmi elles, la plus fréquente concernait les faux dans les titres (6,9% ; moyenne 2020-2024: 11,1%) et/ou l'abus de confiance (3,4% ; moyenne 2020-2024: 5,7%). La proportion de ces infractions préalables dans les communications de soupçons a continué de baisser par rapport aux années précédentes.

Les indications fournies par les intermédiaires financiers sur les infractions préalables présumées constituent une première qualification importante reposant sur les clarifications qu'ils ont effectuées. La fig. 5 ci-dessus présente les infractions que les intermédiaires financiers présument lorsqu'ils sou-

mettent une communication de soupçons. L'analyse faite par le MROS peut aussi établir des soupçons laissant présumer une autre infraction²³.

En 2025, les intermédiaires financiers ont indiqué ne pas être en mesure de mentionner une infraction préalable dans 29% des communications de soupçons. Cette tendance n'a cessé de s'accroître au fil des ans et a de vastes répercussions pour le MROS. Ce dernier doit alors procéder à des clarifications approfondies pour identifier l'infraction préalable.

3.6 Éléments à l'origine des soupçons

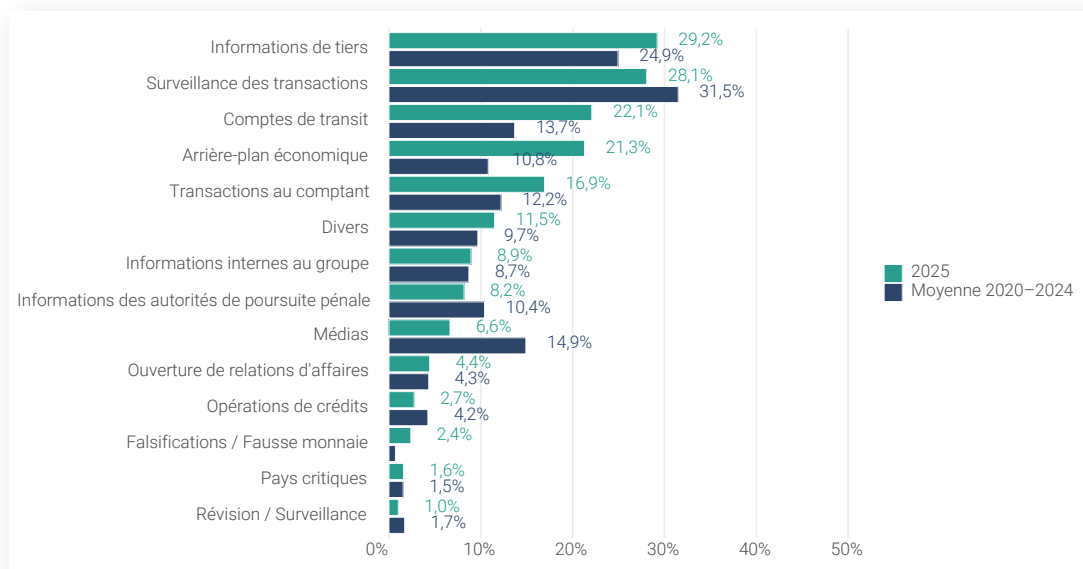
Les communications de soupçons reçues par le MROS reposent en règle générale sur des sources d'informations externes ou des processus de surveillance internes. Durant l'année sous revue, les intermédiaires financiers se sont appuyés sur des informations provenant de tiers dans 29,2% des communications (moyenne 2020-2024: 24,9%) et sur la surveillance des transactions dans 28,1%

²² 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.

²³ Une analyse plus détaillée des diverses infractions préalables au blanchiment d'argent a été effectuée en 2021 sous la direction du GCBF : <https://www.sif.admin.ch/dam/fr/sd-web/zXS66fkBEPEO/zweiter-bericht-risiken-geldwaescherei-terrorismusfinanzierung-fr.pdf>, octobre 2021, pp. 25 à 29.

Fig. 6: Principaux éléments à l'origine des soupçons

2020 – 2025, fréquence, exprimée en % du nombre total de communications (plusieurs réponses possibles)



d'entre elles (moyenne 2020-2024: 31,5%; cf. fig. 6)²⁴. En 2025, d'autres éléments déclencheurs ont pris de l'importance: les comptes de transit ont été cités dans 22,1% des communications, et le manque de clarté de l'arrière-plan économique de la relation d'affaires dans 21,3% d'entre elles (moyenne 2020-2024: 13,7% et 10,8%). Les transactions au comptant ont également été indiquées plus souvent comme élément à l'origine des soupçons (2025: 16,9%, moyenne 2020-2024: 12,2%).

3.7 Dénonciations aux autorités de poursuite pénale

En 2025, le MROS a transmis 1375 dénonciations aux autorités de poursuite pénale en vertu de l'art. 23, al. 4, LBA, ce qui représente une hausse de 31,5% par rapport à l'année précédente (2024:1046). 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'en 2022, une dénonciation reposait en moyenne sur 1,4 communication de soupçons, les dénonciations transmises en 2025 en contenaient 2,2. Ce calcul ne tient pas compte

de quatre cas extraordinaires, dans lesquels plus de 500 communications de soupçons ont été regroupées au sein d'une seule dénonciation.

Les 1375 dénonciations transmises en 2025 contiennent des informations provenant de:

- 4414 communications reçues en 2025, dont 3500 regroupées en quatre dénonciations;
- 1907 communications reçues en 2024;
- 79 communications reçues en 2023;
- 20 communications reçues en 2022;
- 13 communications reçues en 2021;
- 28 communications reçues ou relations d'affaires signalées avant 2021.

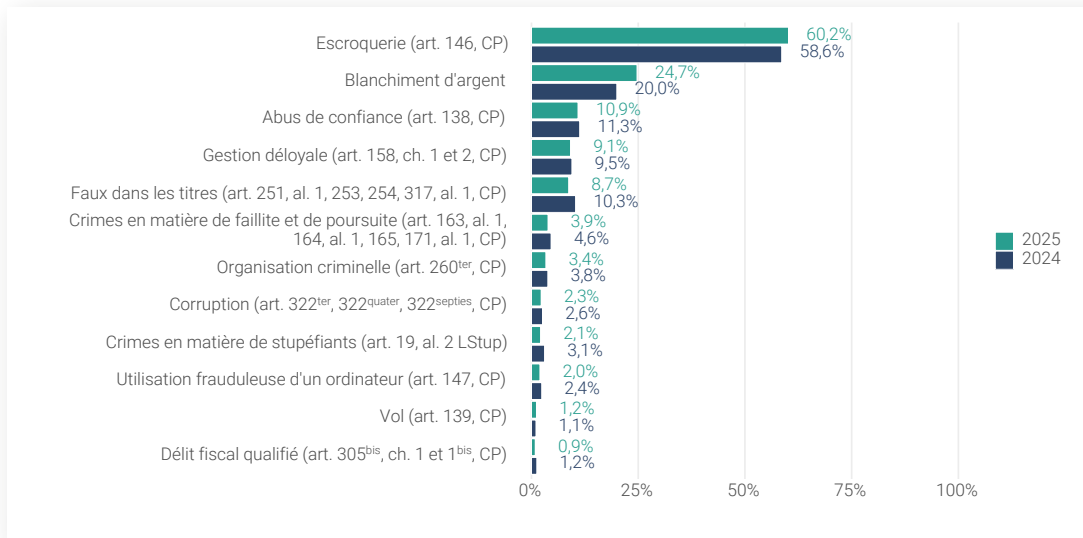
Le MROS a transmis 90,5% de ses dénonciations aux ministères publics cantonaux et 9,5% au Ministère public de la Confédération (MPC). Comme les années précédentes, plus de la moitié des dénonciations ont été déposées auprès d'une poignée seulement de ministères publics cantonaux. Celles déposées à Zurich (15,1%), Vaud (12,7%) et Genève (9,7%) ainsi qu'auprès du MPC (9,5%) représentent près de la moitié de toutes les dénonciations transmises par le MROS (cf. tabl. 2).

²⁴ Dans le système d'information goAML, les intermédiaires financiers peuvent signaler plusieurs éléments qui les ont portés à concevoir des soupçons. Il n'est cependant plus possible d'effectuer une comparaison précise de ces chiffres avec ceux des années antérieures à 2020.

Tabl. 2: Dénonciations transmises par autorité de poursuite pénale 2020–2025

Autorité	2020	2021	2022	2023	2024	2025	2025 en chiffres absolus	Moyenne 2020 – 2025
Zurich	18,9%	21,1%	20,4%	16,3%	17,9%	15,1%	208	18,3%
Vaud	11,1%	11,6%	10,6%	8,3%	12,4%	12,7%	175	11,1%
Genève	11,5%	11,3%	11,6%	17,6%	10,2%	9,7%	134	12,0%
MPC	9,0%	9,1%	6,4%	13,0%	10,3%	9,5%	130	9,6%
Argovie	5,3%	5,2%	6,7%	4,2%	5,7%	8,1%	111	5,9%
Berne	7,5%	6,7%	6,9%	6,5%	7,7%	7,3%	100	7,1%
Fribourg	2,7%	3,1%	2,1%	1,3%	2,1%	4,1%	57	2,6%
Saint-Gall	3,5%	4,0%	6,3%	5,3%	5,3%	4,1%	57	4,8%
Soleure	1,9%	2,0%	2,1%	1,4%	2,1%	3,5%	48	2,2%
Tessin	5,0%	4,8%	3,6%	4,6%	5,5%	3,4%	47	4,5%
Lucerne	3,5%	2,9%	2,6%	2,5%	3,9%	3,3%	45	3,1%
Bâle-Campagne	2,1%	1,7%	2,3%	1,8%	2,2%	2,8%	39	2,1%
Thurgovie	3,0%	2,1%	2,6%	3,2%	1,7%	2,8%	39	2,6%
Valais	2,7%	2,4%	3,0%	2,2%	2,9%	2,7%	37	2,6%
Bâle-Ville	2,6%	2,3%	2,3%	1,8%	3,2%	2,1%	29	2,4%
Neuchâtel	2,3%	1,9%	1,7%	1,3%	1,0%	2,0%	28	1,7%
Zoug	2,5%	2,6%	2,2%	2,2%	1,2%	1,4%	19	2,0%
Schwyz	1,0%	1,1%	1,9%	2,1%	1,5%	1,0%	14	1,4%
Appenzell Rhodes-Extérieures	0,6%	0,8%	1,3%	0,9%	0,5%	0,7%	10	0,8%
Grisons	1,5%	1,0%	1,1%	0,6%	1,1%	0,7%	9	1,0%
Jura	0,3%	1,0%	0,2%	0,7%	0,4%	0,7%	9	0,5%
Nidwald	0,3%	0,4%	0,6%	0,6%	0,3%	0,6%	8	0,5%
Schaffhouse	0,5%	0,5%	0,6%	0,7%	0,6%	0,6%	8	0,6%
Obwald	0,2%	0,1%	0,2%	0,0%	0,2%	0,4%	5	0,2%
Glaris	0,2%	0,1%	0,4%	0,6%	0,2%	0,3%	4	0,3%
Uri	0,3%	0,1%	0,2%	0,1%	0,0%	0,3%	4	0,2%
Appenzell Rhodes-Intérieures	0,0%	0,1%	0,2%	0,2%	0,3%	0,1%	1	0,2%
Total	100,0%	100,0%	100,0%	100,0%	100%	100%	1375	100%

Fig. 7 : Éléments constitutifs d'infraction les plus fréquents dénoncés aux autorités de poursuite pénale
2024 – 2025, fréquence, exprimée en % du nombre total de communications (plusieurs réponses possibles)

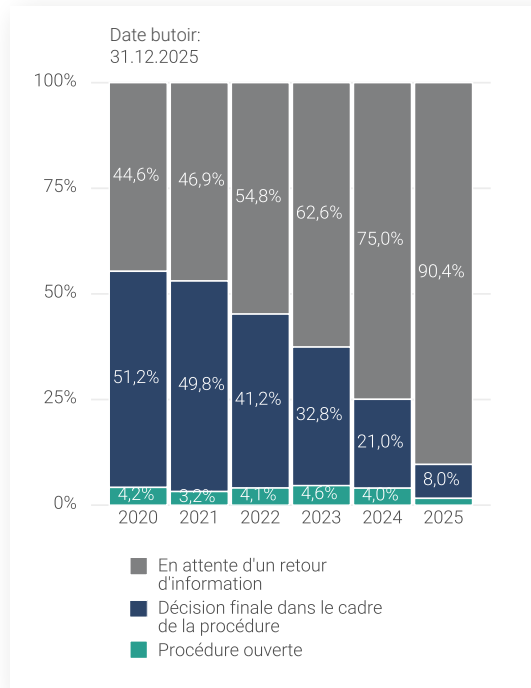


Sur l'ensemble des dénonciations aux autorités de poursuite pénale en 2025, le MROS a suspecté le plus souvent l'escoquerie comme infraction préalable, que ce soit à lui seul ou en combinaison avec d'autres infractions (60,2%, cf. fig. 7). Près d'un dixième des 1375 dénonciations faisaient état d'un soupçon fondé d'abus de confiance (10,9%) et/ou de gestion déloyale (9,1%). Dans près d'un quart des dénonciations, le MROS a indiqué le blanchiment d'argent comme élément constitutif de l'infraction, par exemple dans les configurations où la personne accusée d'avoir commis l'infraction préalable n'était pas la même que celle qui avait commis les actes relevant du blanchiment d'argent.

3.8 Retour d'information des autorités pénales

Conformément à l'art. 29a LBA, les autorités pénales sont tenues de fournir des informations au MROS sur les procédures pendantes en rapport notamment avec le blanchiment d'argent, les organisations criminelles et terroristes et le financement du terrorisme²⁵. De plus, elles l'informent des

Fig. 8 : Retour d'information et état au 31 décembre des dénonciations transmises au cours de l'année
2020 – 2025



²⁵ « 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, RS 311.0. Elles lui font parvenir sans délai les jugements et les décisions de non-lieu correspondants, y compris leur motivation. » (art. 29a, al. 1, LBA)

décisions qu'elles ont prises sur les dénonciations qu'il leur a adressées²⁶. Ce retour d'information est essentiel pour le MROS dans le cadre de l'assistance qu'il apporte aux autorités de poursuite pénale.

Les statistiques du rapport annuel 2024 montrent que le MROS n'a pas encore reçu de retours d'information pour une part considérable des dénonciations, ce qui s'explique notamment par la longueur des procédures pénales²⁷. Au 31 décembre 2024, le MROS n'avait d'informations concernant l'avancement de la procédure que pour 35,7% des cas transmis entre 2020 et 2023. Durant l'année sous revue, le MROS a poursuivi ses efforts pour réduire la proportion de retours d'information en attente, et a cherché à dialoguer avec les autorités de poursuite pénale afin de recevoir les informations prévues par l'art. 29a LBA. En conséquence, le MROS est à présent mieux informé du statut de la procédure dans les cas qu'il a transmis. Au 31 décembre 2025, le MROS avait des informations sur l'avancement de la procédure dans un cas sur deux (49,7%) pour la période allant de 2020 à 2023. Si l'on reprend la méthodologie du rapport annuel 2024 et que l'on considère les dénonciations relatives aux trois années qui, à la date de référence du 31 décembre 2025, remontaient à moins de douze mois (2021-2024), le taux de retour d'information se montait à 46,6% en 2025.

3.9 Financement du terrorisme

En 2025, le MROS a reçu 114 communications relatives à des soupçons de financement du terrorisme, ce qui représente 0,5% de toutes les communications reçues pendant l'année. Dans la plupart des cas, elles sont en outre mises en lien avec d'autres infractions préalables présumées, dont les suivantes sont le plus fréquemment citées :

- appartenance à une organisation criminelle et terroriste²⁸ (31 mentions) ;
- escroquerie²⁹ (16 mentions) ;
- corruption (7 mentions) ;

- infraction à la loi sur les embargos³⁰ (5 mentions) ;
- infraction à la loi sur les stupéfiants³¹ (4 mentions) ;
- faux dans les titres (4 mentions)³².

Les communications relatives à des soupçons de financement du terrorisme proviennent principalement de banques (94) et de prestataires de services de paiement (9).

En 2025, les éléments à l'origine des soupçons suivants sont cités le plus souvent :

- articles de presse (32 mentions) ;
- informations de tiers (29 mentions) ;
- surveillance des transactions (24 mentions) ;
- transactions au comptant (19 mentions) ;
- incertitudes concernant l'arrière-plan économique (17 mentions).

Comme les années précédentes, les communications de soupçons portant sur le financement du terrorisme ont souvent été déclenchées par des articles de presse. Les 114 communications reçues en 2025 ont fait l'objet de cinq dénonciations aux autorités de poursuite pénale compétentes jusqu'au 31 décembre 2025.

3.10 Criminalité organisée

Sur les près de 21 000 communications reçues par le MROS en 2025, les intermédiaires financiers ont indiqué un lien potentiel avec une organisation criminelle dans 695 cas (3,3%). La grande majorité de ces communications de soupçons proviennent du secteur bancaire (77,8%), suivi des prestataires de services de paiement (17,7%). Selon les indications des intermédiaires financiers, ils ont conçu des soupçons à partir d'éléments « divers » dans un tiers des cas (33,7%). Comme éléments spécifiques, ils ont mentionné principalement les informations des médias (25,3%), les transactions au comptant (21,6%) et/ou la surveillance des transactions (17,1% ; cf. Tabl. 3).

²⁶ Art. 29a, al. 2, LBA

²⁷ Cf. [Rapport annuel 2024 du MROS](#), p. 21

²⁸ Art. 260^{ter} CP

²⁹ Art. 146 CP

³⁰ Art. 9, al. 2, de la loi fédérale sur l'application de sanctions internationales (Lemb ; RS 946.231)

³¹ Art. 19, al. 2, de la loi fédérale sur les stupéfiants et les substances psychotropes (LStup ; RS 812.121)

³² Art. 251, ch. 1, 253, 254 et 317, ch. 1, CP

Tabl. 3 : Fréquence des éléments à l'origine des soupçons indiqués dans les communications portant sur des liens présumés avec une organisation criminelle

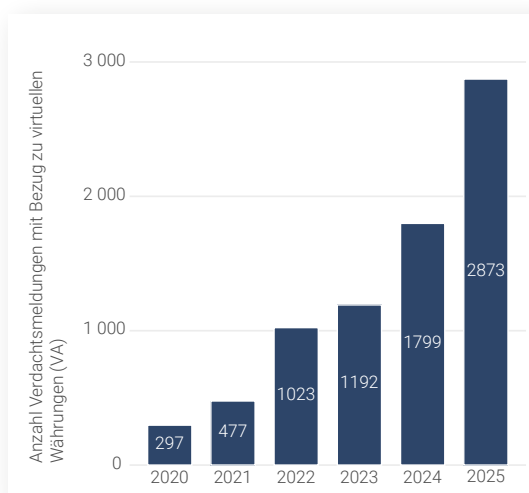
Éléments à l'origine des soupçons (plusieurs réponses possibles, fréquence)	Nombre de mentions	% du nombre total de communications
Divers	234	33,7%
Informations des médias	176	25,3%
Transactions au comptant	150	21,6%
Surveillance des transactions	119	17,1%
Incertitudes concernant l'arrière-plan économique	42	6,0%
Ouverture de relations d'affaires	38	5,5%
Information de tiers	36	5,0%
Information des autorités de poursuite pénale	35	8,0%
Comptes de transit	25	6,8%
Opérations de crédit	23	4,7%

Outre le lien présumé avec une organisation criminelle, les intermédiaires financiers ont souvent mentionné l'escroquerie (53,5%) et/ou le faux dans les titres (17,4%) comme autres infractions préalables possibles. Les 695 communications de soupçons transmises au cours de l'année sous revue, potentiellement en lien avec des organisations criminelles, ont donné lieu à 32 dénonciations aux autorités de poursuite pénale compétentes.

3.11 Communications de soupçons en rapport avec les monnaies virtuelles

En 2025, le MROS a identifié 2873 communications de soupçons en lien avec des monnaies virtuelles (actifs virtuels [AV]³³; cf. fig. 9), ce qui représente une augmentation de 59,7% par rapport à l'année précédente³⁴. Cette évolution pose des défis de plus en plus grands au MROS: avec les monnaies virtuelles, il est beaucoup plus difficile de retracer les flux financiers et donc de trouver l'origine des fonds afin d'identifier clairement l'ayant droit économique. Comme expliqué en détail dans le rapport NRA

« Risque de blanchiment d'argent et de financement du terrorisme lié aux crypto-actifs », publié au premier trimestre de 2024³⁵, les cryptomonnaies présentent des risques accrus.

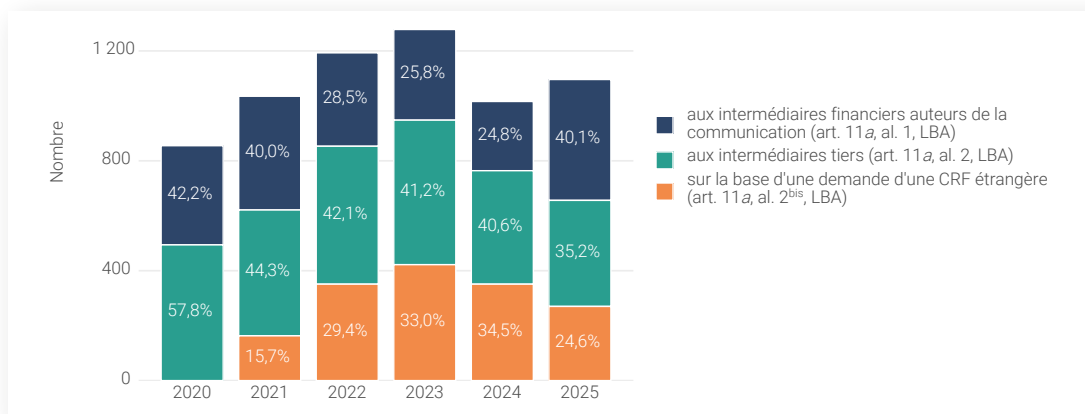
Fig. 9 : Nombre de communications présentant des liens avec des monnaies virtuelles (AV) 2020 – 2025

³³ L'art. 4, al. 2, let. a, de l'ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme (OBA, 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.

³⁴ 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 identifiables de manière inéquivoque. 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'intermédiaires financiers 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.

³⁵ Évaluation nationale des risques (National Risk Assessment, NRA) – [Risque de blanchiment d'argent et de financement du terrorisme lié aux crypto-actifs](#), janvier 2024

Fig. 10 : Demande de remise d'informations au sens de l'art. 11a LBA
2020 – 2025



Depuis le printemps 2024, le MROS recense dans une catégorie distincte (PSAV) les intermédiaires financiers dont l'activité principale est dans le domaine des monnaies virtuelles³⁶. Il peut ainsi en apprendre davantage sur le comportement en matière de communication de cette catégorie d'intermédiaires financiers (cf. tabl. 1). Au 31 décembre 2025, 49 intermédiaires financiers s'étaient enregistrés sous la catégorie PSAV/Fintech sur goAML.

3.12 Remise d'informations en vertu de l'art. 11a LBA

En 2025, le MROS a adressé 1096 demandes d'information à des intermédiaires financiers en vertu de l'art. 11a LBA, ce qui représente une hausse de 7,9% par rapport à l'année précédente (2024 : 1016). En 2024, le nombre de demandes avait reculé pour la première fois depuis 2020, mais il est reparti légèrement à la hausse au cours de l'année sous revue.

Contrairement aux années 2020 à 2024, le MROS a, en 2025, de nouveau adressé plus de demandes

aux intermédiaires financiers auteurs de communications et moins à des intermédiaires tiers : 40,1% des demandes d'information ont été adressées aux intermédiaires financiers initiaux (+15,3% ; art. 11a, al. 1, LBA³⁷, cf. Fig. 10) et 35,2% à des intermédiaires tiers (-5,4% ; art. 11a, al. 2, LBA³⁸), qui prennent ou ont pris part à une transaction ou à une relation d'affaires en plus de l'intermédiaire financier auteur de la communication.

Parmi les demandes d'informations émises par le MROS, près d'une sur quatre découle de l'analyse des informations qu'il a reçues d'un homologue étranger (24,6% ; art. 11a, al. 2^{bis}, LBA³⁹). Pour la première fois depuis l'introduction de l'art. 11a, al. 2^{bis}, LBA en 2021, la proportion de ces demandes a diminué par rapport aux autres types de demandes visées à l'art. 11a LBA (-9,9% par rapport à l'année précédente).

Les demandes d'informations en vertu de l'art. 11a LBA font partie intégrante de l'analyse approfondie effectuée par le MROS en amont de toute transmis-

³⁶ En mars 2024, les intermédiaires financiers enregistrés dans goAML ont été priés de communiquer au MROS s'ils pouvaient être considérés comme des PSAV du fait de leur activité principale.

³⁷ « Lorsque le bureau de communication a besoin d'informations supplémentaires pour l'analyse d'une communication reçue en vertu de l'art. 9 de la présente loi ou de l'art. 305^{ter}, al. 2, CP, l'intermédiaire financier auteur de la communication doit, pour autant qu'il dispose de ces informations, les lui fournir sur demande. » (art. 11a, al. 1, LBA)

³⁸ « 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)

³⁹ « 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)

sion aux autorités de poursuite pénale. En 2025, une dénonciation sur cinq (20,1%) du MROS à une autorité de poursuite pénale était fondée sur des informations et des renseignements obtenus à la suite d'une demande en vertu de l'art. 11a LBA. Selon la complexité du cas, la dénonciation contenait des informations provenant de demandes adressées à plusieurs intermédiaires financiers.

3.13 Annonces de rupture de la relation d'affaires en vertu de l'art. 9b LBA

Depuis le 1^{er} janvier 2023, les intermédiaires financiers peuvent, en vertu de l'art. 9b LBA⁴⁰, rompre la relation d'affaires 40 jours ouvrables après l'avoir signalée au MROS, pour autant que ce dernier ne leur notifie pas qu'il transmet les informations communiquées à une autorité de poursuite pénale. L'intermédiaire financier doit annoncer sans délai au MROS la rupture de la relation d'affaires⁴¹.

Après la forte hausse constatée en 2024, les annonces de rupture de la relation d'affaires se sont stabilisées en 2025: le MROS a reçu 7770 annonces de rupture de la relation d'affaires, soit 9,2% de plus que l'année précédente (cf. Fig. 11). 7,6% 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 2025.

Depuis l'automne 2025, les intermédiaires financiers peuvent, sous certaines conditions⁴², annoncer au MROS directement dans la communication de soupçons leur intention de rompre la relation d'affaires à l'expiration du délai de 40 jours ouvrables. 1462 communications de soupçons comportaient une telle indication.

3.14 Échange d'informations avec les CRF étrangères

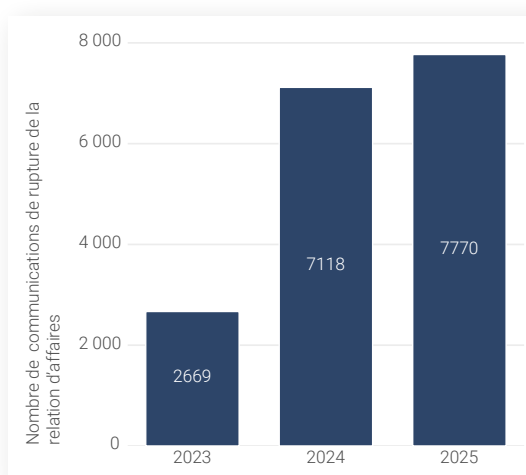
Dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, le financement du terrorisme et la criminalité organi-

sée, l'échange d'informations entre le MROS et les CRF étrangères fonctionne par le biais de l'assistance administrative et constitue un pilier essentiel de cette lutte. Ces informations sont d'une importance capitale pour le travail d'analyse du MROS, car une part considérable des communications de soupçons déposées par des intermédiaires financiers suisses ont un lien avec l'étranger⁴³.

En 2025, le MROS a adressé 237 demandes d'informations à des CRF étrangères, ce qui représente un léger recul de 0,8% par rapport à l'année précédente. À l'inverse, il a reçu au cours de l'année 660 demandes provenant de 91 CRF étrangères (-15,1% par rapport à l'année précédente). Il a traité 323 d'entre elles, ainsi que 99 demandes de l'année précédente.

En revanche, l'échange spontané d'informations entre le MROS et d'autres CRF s'est intensifié. Les CRF étrangères et le MROS peuvent en effet échanger spontanément des informations sans demande préalable, qu'il s'agisse d'une information provenant de l'étranger ayant un lien avec la Suisse ou d'une information que le MROS transmet à une CRF étran-

Fig. 11 : Nombre d'annonces de rupture de la relation d'affaires
2023 – 2025



⁴⁰ En vertu de l'art. 9b LBA, les intermédiaires financiers peuvent rompre une relation d'affaires annoncée 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.

⁴¹ Art. 9b, al. 3, LBA

⁴² Voir chapitre 5.1.

⁴³ [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

gère. En 2025, le MROS a reçu 932 informations spontanées de 56 pays, soit 24,1% de plus qu'en 2024 (751 de 45 pays), et il a envoyé 223 informations spontanées à 53 CRF étrangères, soit 6,6% de plus qu'en 2024 (189 à 41 CRF).

3.15 Échange d'informations avec les autorités suisses

Le MROS échange également, sur demande ou spontanément, des informations pertinentes avec les autorités suisses visées à 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 terrorisme⁴⁴. Au cours de l'année sous revue, le MROS a reçu 498 demandes d'informations provenant de 46 autorités suisses concernant des comptes bancaires, des personnes ou des entreprises spécifiques, soit 11,4% de plus que l'année précédente (2024: 447). Près de trois demandes sur quatre émanaient d'autorités policières. À l'inverse, le MROS a adressé 47 demandes à 15 autorités suisses en 2025, et il a transmis des informations spontanées à des autorités de surveillance et autres autorités suisses dans 490 cas, soit 36,9% de plus (2024: 358)⁴⁵. Il a reçu 120 informations spontanées d'autorités suisses, soit 13,2% de plus (2024: 106).

⁴⁴ 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.

⁴⁵ Dans 72 cas, le MROS a en outre transmis des informations complémentaires aux autorités de poursuite pénale après qu'une dénonciation avait déjà été déposée.

4 Tendances

Ce point consacré aux «Tendances» du présent rapport annuel suit la nouvelle orientation adoptée l'an dernier et remplace désormais le point «Typologies», celles-ci étant publiées sur la page d'accueil du MROS depuis mai 2025. L'analyse des tendances permet de dresser un tableau consolidé et transversal des constatations du MROS, afin de pouvoir mieux appréhender les évolutions dans le domaine du blanchiment d'argent et du financement du terrorisme. Durant l'année sous revue, trois phénomènes se distinguent par une forte dynamique, une internationalisation croissante et des défis particulièrement complexes pour les intermédiaires financiers: l'escroquerie par piratage de la messagerie en entreprise, qui est une forme de fraude toujours aussi largement répandue avec un fort potentiel de nuisance; les «flottes fantômes» liées au contournement de sanctions et enfin, les activités de la mafia italienne, dont les structures et les flux financiers occupent une place importante sur la place financière suisse.

4.1 Escroquerie par piratage de la messagerie en entreprise

L'escroquerie par le biais de l'imitation de messages au sein d'une entreprise est une forme de fraude établie qui se professionnalise de plus en plus. Les sommes dérobées par ce moyen atteignent régulièrement plusieurs millions. Les escrocs se répartissent les tâches et effectuent un travail préparatoire important, si bien qu'ils parviennent à tromper même des collaborateurs expérimentés et qualifiés.

Le mode opératoire est complexe et soigneusement planifié. Les escrocs commencent par analyser les structures internes des entreprises ciblées pendant une longue période, s'intéressant aussi aux processus de décision, aux canaux de communication et à l'organisation hiérarchique. Ils se servent souvent des informations publiques comme les rapports de gestion, les inscriptions au registre du commerce ou les contenus postés sur les réseaux sociaux. L'étape suivante consiste à usurper ou à compromettre l'identité d'un cadre ou d'un partenaire commercial, par le recours à des techniques d'usurpation d'identité (*spoofing*) ou par l'accès indu à des comptes e-mail légitimes. Les collaborateurs concernés reçoivent alors de fausses instructions de paiement ressemblant à s'y méprendre

aux vraies qu'ils reçoivent d'ordinaire, mais l'argent viré est envoyé sur des comptes contrôlés par les escrocs. La Suisse, en raison de son tissu économique fortement axé sur l'international, notamment dans le domaine des petites et moyennes entreprises, est une cible particulièrement attractive pour des agissements de ce type. Des formes d'organisation légères, des hiérarchies claires et une confiance traditionnellement élevée dans la communication interne favorisent le succès de cette tromperie. Du fait du plurilinguisme, les anomalies linguistiques subtiles sont en outre plus difficiles à repérer dans les e-mails.

À cet égard, le MROS constate deux types de flux de communication et d'information: d'une part, il reçoit des communications de soupçons identifiant les comptes des auteurs présumés ou des demandes d'autorités de poursuite pénale suisses ayant besoin d'informations de la part de CRF étrangères. D'autre part, il reçoit des demandes urgentes de CRF étrangères visant à faire immédiatement bloquer des transactions ou des comptes. Dans ce cas, il importe d'agir immédiatement: tout retard, notamment en raison des problèmes d'attribution des compétences des autorités impliquées, peut se traduire par un échec parce que les fonds sont rapidement transférés à l'étranger ou changés en argent liquide.

Des expériences positives ont été faites avec le réseau international des CRF dans des cas de ce type. Même si les communications ne sont souvent déposées qu'après l'exécution de la transaction, les CRF étrangères fournissent en règle générale vite les informations requises pour prendre les mesures suivantes (par ex. une demande d'entraide judiciaire). Dans certains cas, on parvient même à accomplir les démarches nécessaires avant que les fonds ne soient crédités à l'institut étranger via des banques de correspondance. Grâce à la collaboration efficace des personnes lésées, des autorités de poursuite pénale, des CRF et des banques impliquées, il est possible dans de telles configurations de bloquer immédiatement des fonds qui viennent d'être transférés.

À titre d'exemple, on peut citer un cas récent de *Business email compromise (BEC fraud)*: une entreprise suisse entretenait une relation commerciale avec une entreprise des Émirats arabes unis.

Dans ce cadre, une facture de plusieurs millions de francs suisses reçue par e-mail paraissait plausible au premier abord. C'est seulement après avoir exécuté le virement que l'entreprise s'est rendu compte de l'escroquerie. L'argent était destiné non pas au partenaire commercial légitime, mais à un compte étranger contrôlé par des escrocs.

L'entreprise lésée a immédiatement pris contact avec la banque afin d'interrompre la transaction déjà exécutée. Dans le même temps, la police compétente a adressé une demande au MROS en le priant de faire bloquer tout de suite la transaction par la CRF des Émirats arabes unis. Depuis l'entrée en vigueur de la *Federal decree law n° 10 (2025)*, celle-ci dispose en effet de pouvoirs plus étendus dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme. Le directeur de la CRF peut suspendre des transactions pendant 10 jours ouvrables au plus (*suspension power*) et geler des fonds ou des valeurs patrimoniales liées à des fonds pendant 30 jours au plus (*freezing power*). En fin de compte, il a été possible d'empêcher le virement aux Émirats arabes unis. Et si les fonds étaient arrivés sur le compte des escrocs, ils auraient été bloqués immédiatement en raison de l'excellente coopération nationale et internationale à tous les niveaux.

En comparaison internationale, on relève qu'en l'état actuel et contrairement à bon nombre de CRF étrangères, le MROS ne dispose pas de pouvoirs légaux propres pour suspendre des transactions ou bloquer des comptes. De telles compétences existent notamment en Belgique, en Italie, en France, aux Pays-Bas, au Luxembourg, en Espagne et au Portugal. Au niveau européen, la Directive (UE) 2024/1640 du 31 mai 2024 exige que d'ici au 10 juillet 2027 au plus tard, toutes les CRF de l'Union européenne soient systématiquement habilitées à suspendre des transactions et à bloquer des comptes. Ces compétences doivent pouvoir être mises en œuvre non seulement en cas de soupçon de blanchiment d'argent ou de financement du terrorisme, mais aussi dans le cadre d'activités purement analytiques⁴⁶. Sur le plan international, on observe une évolution similaire: un nombre croissant de CRF se

voient conférer des pouvoirs élargis pour la saisie immédiate de valeurs patrimoniales d'origine criminelle présumée.

4.2 Flottes fantômes

Ces dernières années, ce terme est apparu de manière récurrente dans les médias. Par « flottes fantômes », on entend des navires ou des flottes entières qui opèrent délibérément hors des mécanismes établis de contrôle, de transparence et de surveillance, notamment afin de contourner des sanctions internationales. Il s'agit souvent de pétroliers ou de cargos vieillissants qui ne sont plus certifiés. En utilisant des données d'enregistrement ou d'immatriculation contradictoires ou qui changent fréquemment⁴⁷ ainsi que des structures de propriété complexes et opaques⁴⁸, on tente de dissimuler la provenance et la destination des biens transportés ainsi que l'identité des ayants droits économiques.

Bien que la Suisse ne dispose d'aucun débouché à la mer, à l'exception d'une liaison indirecte avec la mer du Nord via le Rhin, elle est néanmoins touchée par ce phénomène à plusieurs égards. En tant que place financière de classe internationale, la Suisse possède un grand secteur de négoce de matières premières et d'importantes sociétés d'assurances et de logistique. En outre, certaines des plus grandes compagnies maritimes au monde ont leur siège en Suisse. Le registre suisse de la navigation maritime à Bâle fait office de port d'immatriculation pour de nombreux bateaux de passagers et de croisière circulant sur les voies navigables intérieures européennes. De ce fait, le MROS estime qu'il est important de s'attaquer aux flottes fantômes dans le contexte du contournement de sanctions, notamment en relation avec l'agression militaire russe contre l'Ukraine.

Comme mentionné dans le rapport annuel 2022, la compétence du droit suisse des sanctions incombe au Secrétariat d'État à l'économie (SECO), qui surveille également l'exécution des obligations de déclarer selon ce droit. En cas de violations graves de la loi sur les embargos, la communication d'un intermédiaire financier suisse au MROS peut toute-

⁴⁶ Art. 24 de la Directive (UE) 2024/1640

⁴⁷ Les navires battent souvent des pavillons dits « de complaisance » comme le Panama, les îles Marshall ou le Liberia.

⁴⁸ Souvent des sociétés de domiciles ou des sociétés offshore opaques

fois s'avérer utile, dans la mesure où des indices de blanchiment d'argent ou de financement du terrorisme apparaissent au cours des clarifications relatives à la violation ou au contournement de sanctions⁴⁹.

Le phénomène des flottes fantômes n'est pas nouveau, ni uniquement lié à l'attaque russe contre l'Ukraine. Déjà dans les années 1920, des pétroliers américains battant pavillon panaméen étaient utilisés pour transporter de l'alcool. Au cours des décennies suivantes, la Corée du Nord et l'Iran notamment ont eu recours à des structures de ce type pour pouvoir importer ou exporter des marchandises en dépit des sanctions internationales. La situation sécuritaire actuelle a toutefois entraîné une intensification et une professionnalisation de ces pratiques.

Le MROS constate lui aussi que la question des flottes fantômes est loin d'être anodine pour la place financière suisse. Des intermédiaires financiers suisses ont déposé des communications de soupçons à ce sujet, et des CRF étrangères lui ont fait parvenir des demandes en relation avec le contournement présumé de sanctions. Selon les informations du MROS, il existe divers indicateurs, qui, seuls ou combinés, peuvent laisser penser à un potentiel contournement de sanctions. Il s'agit de :

a. Caractéristiques des navires et équipements techniques

- Les navires concernés sont très anciens.
- Des changements de pavillon sont effectués à courts intervalles.
- Les certificats de maintenance et de sécurité paraissent incomplets, inhabituels ou incohérents.

b. Structure de propriété et d'armateurs

- La structure de propriété est complexe et opaque, impliquant souvent des sociétés écrans et des sociétés offshore.
- Le propriétaire change fréquemment.
- Les sièges des sociétés propriétaires sont situés dans des pays à risque, par exemple en raison de l'absence de registre de transparence.

- Les ayants droits économiques ne sont pas identifiés de façon définitive et/ou sont dissimulés derrière des architectures opaques.

c. Schéma commercial et routes

- Les routes choisies paraissent inhabituelles ou non plausibles du point de vue économique (par ex. impliquant de longs détours).
- Il y a de fréquents changements de cap ou arrêts dans des zones marines connues pour la présence de flottes fantômes.
- Il y a une combinaison de destinations légales et de destinations sous sanctions.

d. Situation du fret et documentation

- Les informations sur la provenance, le type et la quantité du chargement sont contradictoires ou incomplètes.
- Les certificats d'origine ou les documents d'accompagnement indiquent l'exportation potentielle depuis des pays sous sanctions, le cas échéant via des pays tiers.
- Il y a une disproportion entre le chargement déclaré et la taille ou la capacité du navire.

e. Structures et flux financiers

- Les flux financiers sont organisés de manière complexe et passent par plusieurs instituts financiers, comprenant souvent des banques situées dans des centres offshore.
- Il y a des indices de blanchiment de capitaux basé sur le commerce (*Tradebased Money Laundering, TBML*) par exemple par le biais de la sur- ou la sous-évaluation des marchandises.
- Des paiements sont effectués par des sociétés sans activité commerciale clairement identifiable.

f. Liens avec les sanctions et les risques

- Il existe des liens directs ou indirects avec des pays frappés par des sanctions.
- Des ports sont utilisés dans lesquels les contrôles sont faibles ou insuffisants.
- Les noms de compagnies maritimes ou d'assureurs classés à haut risque apparaissent.
- Des navires, des entreprises ou des personnes figurent sur des listes de sanctions ou de surveillance (*watchlist*).

⁴⁹ Droit de communiquer (art. 305^{er}, al. 2, CP) ou obligation de communiquer (art. 9 LBA)

Cette liste n'est pas exhaustive et donne simplement quelques exemples d'indicateurs qui peuvent être le signe de graves violations potentielles de la LEmb et déclencher l'envoi d'une communication de soupçons au MROS.

4.3 Mafia italienne

Les organisations mafieuses italiennes sont impliquées dans une grande variété d'activités criminelles, englobant à la fois les infractions classiques et les formes modernes de criminalité financière et économique. Leur revenu principal provient toujours et encore du trafic international de stupéfiants, qui constitue le pilier économique de ces organisations. D'autres champs d'action prééminents sont le trafic d'armes, la traite des êtres humains et le trafic des déchets, qui s'étend à toute l'Italie et au-delà, jusqu'en Europe de l'Est et en Afrique du Nord. On peut encore y ajouter la corruption et diverses formes de prise d'influence systématique sur des structures et des processus de l'État, par exemple en lien avec les marchés publics. En parallèle, ces organisations mafieuses ne cessent de développer leurs activités dans le domaine de la criminalité économique moderne, ce qui englobe les cyber-infractions, les fraudes à l'investissement et à l'assurance, les faillites frauduleuses et les manipulations de marché. Enfin, le trafic de produits de contrefaçon et l'extorsion de fonds (aux fins de contrôler un territoire) complètent ce système axé sur la domination, l'influence et le profit.

Il est difficile de savoir avec certitude à combien s'élèvent les chiffres d'affaires de la mafia italienne. Selon diverses études, les recettes annuelles des organisations mafieuses italiennes atteindraient entre 40⁵⁰ et 150 milliards⁵¹ d'euros par an. De tels montants rendent d'autant plus impérieuse leur nécessité d'injecter ces fonds dans le circuit économique légal pour pouvoir les réinvestir dans des activités d'entreprises légales ou dans le secteur immobilier.

Toutes les grandes organisations de la mafia italienne sont présentes en Suisse: la 'Ndrangheta de

Calabre, la Camorra de Campanie, la Cosa Nostra de Sicile, et la Sacra Corona Unita des Pouilles. De plus, des membres de la Criminalità barese et de la Società foggiana, également des Pouilles, sont aussi actifs en Suisse. Parmi tous ces groupes, la 'Ndrangheta est particulièrement bien implantée dans notre pays. Ces organisations criminelles ne limitent pas leurs activités à la simple gestion de fortune ou au blanchiment d'argent. Elles cherchent plutôt à s'infiltrer et à prendre de l'influence sur les structures économiques et sociétales à moyen et à long terme. Des individus connus pour leur proximité avec des organisations mafieuses vivent en Suisse, sont bien intégrés professionnellement et se comportent avec discrétion. Cette intégration sociale est une caractéristique centrale des structures mafieuses qui les distingue d'autres formes de criminalité organisée⁵².

En Suisse, le blanchiment d'argent n'est qu'une des nombreuses activités de la mafia italienne. Parmi les domaines d'infraction constatés, on compte notamment le trafic de stupéfiants, le trafic d'armes, l'assistance à des personnes recherchées par la police, le chantage, les homicides, la traite des êtres humains aux fins d'exploitation sexuelle ou d'exploitation de la force de travail, la contrebande de denrées alimentaires, les faillites frauduleuses, la fraude à l'investissement, la fraude à l'assurance, le trafic de fausse monnaie et les jeux de hasard illégaux. L'infiltration de l'économie légale traverse de nombreux secteurs, touchant notamment l'immobilier, la construction, l'hôtellerie-restauration, l'alimentation, le commerce de détail, la gestion des déchets, l'approvisionnement énergétique, les fiduciaires, les cabinets d'avocats et les études de notaires, les entreprises de technologie et d'informatique, les jeux en ligne, les agences de voyage, les pompes funèbres et le secteur automobile. N'importe quel secteur économique peut être ciblé par ces activités. L'accès est souvent procuré par des prête-noms ou des intermédiaires formels discrets, le but étant d'influencer les mécanismes de marché et les processus de décision.

⁵⁰ <https://aliautonomie.it/2025/01/13/legalita-cgia-le-mafie-hanno-volume-daffari-da-40-miliardi-anno-in-italia-150mili-impese-nellorbita-della-criminalita/> (en italien uniquement)

⁵¹ www.ilsole24ore.com/art/cosi-mafia-ha-messo-mani-cio-che-mangiamo-AEd82reG (en italien uniquement)

⁵² <https://direzioneeinvestigativaantimafia.interno.gov.it/relazioni-semestrali/>, rapport 2024, p. 341

Le MROS constate que dans de nombreux cas, les valeurs patrimoniales acquises par des moyens délictueux ont déjà été injectées dans le circuit financier légal à l'étranger, avant d'être transférées sur des comptes en Suisse par transaction électronique. Le recours à de fausses factures, à des sociétés offshore et à des structures de paiement complexes est fréquent, et ces fonds sont souvent mélangés avec des revenus légaux. En outre, l'utilisation d'argent liquide présente toujours un potentiel de blanchiment non négligeable, étant donné que les obligations de diligence légales ne s'appliquent qu'à partir d'un certain seuil. Ces conditions encouragent les organisations criminelles à effectuer des transactions au comptant, notamment en lien avec le trafic de stupéfiants, la traite des êtres humains ou les infractions contre la propriété.

Un autre élément de poids est le rôle joué par la Suisse dans le commerce international et le raffinage de l'or. La Suisse traite une part considérable de la production aurifère mondiale. Malgré les prescriptions réglementaires sur le contrôle de l'importation et la traçabilité, il n'en reste pas moins difficile de vérifier sans lacune l'origine réelle de l'or. La combinaison entre de grands volumes de transactions, un réseau global et des possibilités de contrôle parfois réduites rend ce secteur attractif aussi pour les organisations mafieuses, qui sont tentées d'y investir des valeurs patrimoniales acquises par des moyens délictueux⁵³.

Le MROS renforce son engagement dans la lutte contre le blanchiment d'argent en relation avec les activités d'organisations criminelles. La participation à une organisation criminelle est punissable d'une peine privative de liberté de dix ans au plus, conformément à l'art. 260^{ter} CP. Si les éléments constitutifs de l'infraction sont donnés, il s'agit d'un crime pouvant constituer une infraction préalable au blanchiment d'argent. Plusieurs cas importants ont été découverts : cette priorité correspond à la stratégie 2024-2027 de fedpol et du MROS⁵⁴. Ces dernières années, près de 5% des communications

de soupçons reçues par le MROS faisaient état de liens avec des organisations criminelles. L'analyse approfondie révèle toutefois souvent que les conditions légales de l'art. 260^{ter} ne sont pas remplies. À l'inverse, lors du traitement de communications de soupçons déposées initialement pour d'autres motifs, il n'est pas rare qu'apparaissent des indices de liens potentiels avec des organisations criminelles. Les acteurs intermédiaires comme les fiduciaires, les avocats et les gestionnaires de fortune jouent un rôle essentiel à cet égard. Des zones de prédilection pour ces agissements ont été mises en évidence notamment au Tessin, à Grono (GR), en Valais et dans des centres urbains comme Zurich et Bâle ; mais la Suisse entière est touchée.

En 2025, le MROS a transmis pour la première fois un cas de soupçons de blanchiment d'argent en relation avec une violation potentielle de l'art. 60, al. 1^{bis}, de la loi fédérale sur la protection de l'environnement⁵⁵, un domaine d'infraction typiquement associé aux activités mafieuses. Depuis l'entrée en vigueur de la loi révisée le 1^{er} avril 2025, cette infraction contre l'environnement peut être considérée comme un crime, et peut donc constituer une infraction préalable au blanchiment d'argent.

Les connexions avec des organisations criminelles sont généralement difficiles à identifier. De nombreuses infractions sont commises à l'étranger et l'intégration sociale des acteurs impliqués les rend encore plus difficile à repérer et à démasquer. Il y a une multitude d'indicateurs à prendre en compte dans l'analyse et il faut pouvoir compter sur une coopération internationale étroite. Ces dernières années, le MROS a notamment intensifié sa coopération avec le MPC, la Police judiciaire fédérale, la CRF italienne et Europol, afin de renforcer l'échange d'informations et de développer des approches stratégiques communes.

⁵³ Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, 2015, pp. 101-102, www.news.admin.ch/newsd/message/attachments/39966.pdf OFDF, Rapport annuel Commerce extérieur suisse 2023, pp. 30-35, www.bazg.admin.ch/dam/fr/sd-web/Glgl.22f5YT1m/912.5-02%20jb%202023_1.1_fr.pdf

⁵⁴ <https://www.fedpol.admin.ch/dam/fr/sd-web/ux-P5UbpjIB7/strategie-mros.pdf>, www.news.admin.ch/fr/nsb?id=103191, <https://fedpol-ok.ch/fr>, www.swissinfo.ch/eng/swiss-politics/fighting-organized-crime-with-a-national-strategy/88241703 (en anglais uniquement)

⁵⁵ (LPE; RS 814.01)

5 Pratique du MROS

5.1 Changement de pratique : annonces de rupture selon la règle de *minimis*

Depuis l'entrée en vigueur de l'art. 9b LBA au 1^{er} janvier 2023, les intermédiaires financiers ont la possibilité de rompre une relation d'affaires qui fait l'objet d'une communication de soupçons après un délai de 40 jours ouvrables, pour autant que le MROS n'ait pas fait suivre les informations transmises à une autorité de poursuite pénale.

L'application de cette disposition dans la pratique montre qu'une part considérable des relations d'affaires concernées ne présentaient que des montants modestes sur leur compte au moment de la communication, et que souvent le compte était soldé après l'expiration du délai légal. Dans de telles configurations, l'annonce de rupture prévue par la loi et intervenant en aval n'a souvent pas apporté de gain d'informations supplémentaires, mais a surtout généré du travail administratif supplémentaire pour les intermédiaires financiers et le MROS. C'est pourquoi le MROS a introduit une pratique simplifiée en 2025 : « la pratique de *minimis* en matière de notification de rupture » Cette modification a pour but de rendre les flux de communications plus efficaces dans des cas clairement délimités et de décharger les acteurs concernés sur le plan administratif. La nouvelle pratique a été communiquée en août 2025 par une newsletter aux intermédiaires financiers.

5.1.1 Éléments clés de cette nouvelle pratique

La pratique de *minimis* permet aux intermédiaires financiers d'annoncer la rupture prévue d'une relation d'affaires déjà au moment d'envoyer la communication de soupçons, pour autant que les conditions cumulatives suivantes soient remplies :

- **Valeurs patrimoniales de faible valeur :** l'avoit total de la relation d'affaires doit être inférieur à 15000 CHF au moment de la communication de soupçons.
- **Intention irrévocable de rupture :** au moment de la communication de soupçons, l'intermédiaire financier s'engage par écrit à rompre la relation d'affaires après expiration d'un délai de 40 jours ouvrables conformément à l'art. 9b LBA.
- **Mention dans la communication de soupçons :** la rupture est signalée par l'inscription du code **CANC40** dans le deuxième champ (« raisons des soupçons »). Ce code se réfère à toutes les relations d'affaires mentionnées dans la communication de soupçons.

Si la rupture est annoncée à l'avance de cette manière, il n'est plus nécessaire de faire d'annonce de rupture séparée par la suite. Le MROS marque ces communications à l'interne. Conformément à l'art. 11a LBA, il fera lui-même une demande s'il a besoin d'informations supplémentaires pour son analyse.

5.1.2 Limites juridiques et pratiques de l'annonce de rupture préalable

Les retours des intermédiaires financiers ainsi que les premières expériences du MROS depuis l'introduction de cette nouvelle pratique montrent qu'il est difficile de prévoir à l'avance comment une relation d'affaires va se dérouler entre le dépôt de la communication de soupçons et la clôture définitive du compte.

Divers aspects doivent être pris en considération :

- **Mouvements de fonds pendant le délai de 40 jours :** les transactions entreprises avant l'échéance du délai ne peuvent pas être exclues. Même des entrées ou des sorties d'argent minimes peuvent avoir une importance pour l'analyse.
- **Retards dans la clôture effective :** la fermeture effective du compte peut être reportée, par exemple si le client n'indique pas de nouvelle relation bancaire ou s'il existe des obstacles d'ordre opérationnel qui empêchent la clôture.
- **Versement du solde en espèces :** le versement du solde en espèces est possible, mais seulement s'il s'agit de petits montants.

Jusqu'à la fermeture du compte, l'intermédiaire financier est tenu d'exercer son devoir de diligence sans restriction. Il doit notamment effectuer un monitoring fondé sur les risques de la relation d'affaires et déposer de nouvelles communications de soupçons en cas de convergence supplémentaire de soupçons ou de l'apparition de nouveaux éléments significatifs. Selon les cas, une nouvelle obligation de communiquer peut en découler, indépendamment de la communication initiale.

L'introduction de « la pratique de *minimis* en matière de notification de rupture » vise à simplifier le processus de communication dans certaines configurations clairement définies impliquant des montants modestes. Cette règle réduit les communications redondantes et allège la charge adminis-

trative des intermédiaires financiers et du MROS, sans compromettre la qualité de l'analyse de blanchiment d'argent. En outre, dans les cas au risque élevé ou relevant potentiellement du droit pénal, il reste garanti que toutes les informations requises pourront être recueillies et soumises à un examen minutieux avant d'être transmises.

5.2 Normes en matière de données

5.2.1 Normes en matière de données pour les communications de soupçons

En raison de la hausse constante du nombre de communications de soupçons, la question de la qualité des données a pris encore davantage d'importance durant l'année sous revue. Les manques qualitatifs existants se sont aggravés, si bien que le MROS a régulièrement dû retourner à l'expéditeur des communications ou des pièces jointes, notamment en raison de champs obligatoires incomplets, de formats de données non conformes ou d'indications non structurées. Ces renvois ont généré une charge administrative supplémentaire et des retards pour les intermédiaires financiers auteurs de communications, sans compter qu'ils ont aussi nuï à l'efficacité du traitement et de l'analyse des informations par le MROS.

5.2.2 Nouveauté législative : l'art. 23, al. 7, LBA

La dernière révision de la LBA a tenu compte de ce problème, en créant une nouvelle base légale qui entrera en vigueur à l'été 2026. Le nouvel art. 23, al. 7, LBA stipule que l'échange(de données) avec le MROS doit impérativement passer par le système d'information de ce dernier et habilite fedpol à édicter des prescriptions contraignantes sur les normes à respecter en matière de données pour les informations transmises via goAML. Cette disposition constitue pour la première fois une base légale explicite qui régleme des exigences formelles et structurelles relatives à l'échange électronique d'informations. Conçues jusqu'ici comme des recommandations spécialisées, les spécifications techniques du MROS, notamment celles contenues dans le manuel d'utilisation du système goAML et du fichier XML associé, se voient désormais conférer un caractère contraignant. Elles s'appliquent désormais à tous les acteurs soumis à l'obligation de communiquer, à savoir les intermédiaires financiers, les conseillers et les négociants, mais aussi aux autorités qui communiquent avec le MROS.

Cette règle vise à garantir durablement l'uniformité, l'intégralité et la qualité formelle des communications de soupçons.

5.2.3 Mise en œuvre technique : procédés et perspective

Sur la base de l'art. 23, al. 7, LBA, fedpol va élaborer une ordonnance technique qui concrétisera en détail les exigences en matière de données fixées par les nouvelles normes. Cette ordonnance reprendra les spécifications existantes, à savoir celles du manuel goAML et du fichier XML actuel, qui constituent un cadre de référence aujourd'hui déjà et sont appliquées par une grande partie des acteurs soumis à l'obligation de communiquer.

L'établissement de ces normes vise notamment à réduire le nombre de communications présentant des lacunes formelles et les retours à l'expéditeur qui en découlent, tout en soulageant durablement le MROS. Par ailleurs, la standardisation contribue à renforcer la sécurité du droit et l'égalité de traitement pour tous les acteurs soumis à l'obligation de communiquer. À long terme, une réglementation claire et contraignante sur la qualité des données garantira un traitement automatisé plus efficace; un meilleur suivi des communications et des informations complémentaires; des analyses plus fiables de la part du MROS et une transmission plus efficace aux autorités de poursuite pénale et aux autorités partenaires étrangères. Globalement, l'introduction d'une norme uniforme et contraignante en matière de données rend le dispositif suisse de lutte contre le blanchiment d'argent plus performant.

5.2.4 XML Data Quality Report

En complément de la norme en matière de données, le MROS développe l'outil XML Data Quality Report. La version 1.0 d'XML Data Quality Report servira à mesurer automatiquement la qualité des données dans les communications de soupçons reçues et à la surveiller de manière systématique.

Sur cette base, il est prévu que les intermédiaires financiers reçoivent à intervalles réguliers des rapports standardisés sur la qualité des données (*DQ reports*). Ces rapports détailleront l'état et l'évolution de la qualité des données contenues dans les communications transmises et permettront d'effectuer un classement par rapport aux valeurs de

comparaison agrégées. Ces rapports serviront exclusivement à garantir la qualité et aideront les intermédiaires financiers à développer leurs processus internes de communication de manière ciblée. Dans la version 1.0 d'XML Data Quality Report, le MROS a défini différentes valeurs pour mesurer la qualité des données. Le choix a été opéré sur la base de l'influence de la qualité sur les processus d'analyse et du potentiel d'automatisation. De premiers essais avec un nombre réduit d'intermédiaires financiers sont prévus au premier trimestre 2026. À l'issue de la phase de test, le MROS prévoit de mettre les *DQ reports* à la disposition de tous les intermédiaires financiers à partir de l'été 2026.

Avec XML Data Quality Report, on introduit pour la première fois un outil uniforme, comparable et permanent qui évalue la qualité des données au niveau de chaque intermédiaire financier. La garantie durable d'une qualité formelle élevée des communications de soupçons permettra au MROS de travailler de manière plus efficiente.

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

La lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération requière une coopération internationale efficace. Le MROS collabore au sein de forums multilatéraux et bilatéraux et participe à l'échange international d'informations et d'expériences tant au niveau opérationnel que stratégique.

6.1 Groupe Egmont

Le Groupe Egmont est le réseau mondial des CRF. Il compte actuellement 182 membres et sert à l'échange structuré d'informations, de méthodes et d'expertise.

Le Groupe Egmont a organisé ses 25^e réunions annuelles des groupes de travail et groupes régionaux du 27 janvier au 8 février 2025. Les séances se sont déroulées sous forme virtuelle. Plus de 800 représentants des CRF, des organisations internationales partenaires et des observateurs y ont pris part. Les discussions ont porté notamment sur des questions d'échange d'informations opérationnel, sur des aspects d'efficacité et sur l'utilisation de nouvelles technologies.

La 30^e assemblée plénière du groupe Egmont a eu lieu du 6 au 11 juillet 2025 au Luxembourg. Organisée par la CRF luxembourgeoise, elle a inscrit à l'ordre du jour des questions touchant au développement de la coopération internationale entre CRF dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Des représentants d'autorités nationales et internationales ont également participé à cette assemblée. Plusieurs interventions ont traité de l'importance de la coopération internationale dans la lutte contre la criminalité financière⁵⁶.

Le MROS a participé aux travaux du Groupe Egmont durant l'année sous revue. Une réunion organisée en collaboration avec ECOFEL a eu lieu à Berne les 14 et 15 octobre 2025 (cf. ch. 2.7.1). La cheffe suppléante du MROS a assumé sa fonction de repré-

sentante régionale de la région Europe II au sein du comité Egmont. Cette région englobe notamment les CRF du Royaume-Uni, de Monaco, des îles Anglo-Normandes, d'Israël, de Géorgie et d'Ukraine.

6.2 Groupe d'action financière (GAFI)

Le GAFI⁵⁷ a poursuivi ses travaux en 2025 en vue de développer des normes internationales visant à lutter contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération.

La réunion annuelle des experts (*Joint Expert Meeting, JEM*) s'est déroulée début 2025 à Vienne. Les travaux ont porté sur les thèmes du recouvrement d'avoirs (*asset recovery*) et du financement du terrorisme.

Du 19 au 21 février 2025, le GAFI a tenu sa première réunion plénière de l'année à Paris. Des délégations du réseau global du GAFI et des organisations internationales observatrices ont participé aux discussions⁵⁸. La plénière a notamment convenu de modifications des normes du GAFI afin de mieux soutenir l'approche fondée sur les risques et l'inclusion financière et a adopté un rapport sur les flux financiers en rapport avec l'exploitation sexuelle des enfants en ligne⁵⁹.

Les 12 et 13 juin 2025 s'est déroulée une réunion plénière conjointe avec Moneyval, l'organe d'évaluation du Conseil de l'Europe pour les États membres qui ne font pas partie du GAFI. Dans un but de transparence, les participants ont décidé notamment de modifier la recommandation 16 afin d'améliorer la sûreté et la sécurité des paiements transfrontaliers. Désormais, pour les transactions internationales de plus de 1000 dollars américains ou euros, des informations précises sur le donneur d'ordre et le bénéficiaire sont requises. Les intermédiaires financiers doivent mettre en œuvre ces exigences d'ici à 2030 au plus tard⁶⁰.

La troisième réunion plénière de l'année a eu lieu du 22 au 24 octobre 2025 à Paris. Le GAFI y a no-

⁵⁶ [L'unité de renseignement financier luxembourgeoise \(CRF\) accueille le 30e anniversaire du groupe Egmont lors de sa séance plénière annuelle](#)

⁵⁷ Pour davantage d'informations sur la structure et les tâches de l'organisation, cf. [Rapport annuel MROS 2023](#), ch. 7.2

⁵⁸ [Résultats de la plénière du GAFI, 19-21 février 2025](#)

⁵⁹ [Détecter, perturber et enquêter sur l'exploitation sexuelle des enfants en ligne](#)

⁶⁰ [Résultats de la plénière conjointe GAFI-MONEYVAL, 12-13 juin 2025](#)

tamment adopté les rapports des deux évaluations mutuelles sur la Belgique et la Malaisie.

Durant l'année sous revue, le GAFI a en outre modifié la composition de la « liste grise ». Cette liste comprend les juridictions soumises à une surveillance renforcée qui travaillent activement avec le GAFI pour remédier aux déficiences stratégiques de leur régime de lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération. Le GAFI a nouvellement placé sur cette liste le Laos, le Népal, la Bolivie et les Îles Vierges britanniques. Les pays suivants ont notamment été retirés de la liste : Philippines, Croatie, Mali, Tanzanie, Burkina Faso, Mozambique, Nigéria et Afrique du Sud.

Le GAFI a publié en février 2024 une nouvelle ligne directrice fondée sur les risques pour mettre en œuvre la recommandation 25, intitulée « transparence et bénéficiaires effectifs des constructions juridiques »⁶¹. Dans ce cadre, la Suisse a adopté le 26 septembre 2025 la LTPM. Le registre prévu, qui ne sera pas public, permettra aux autorités compétentes d'accéder à des informations fiables sur les ayants droits économiques d'une entité juridique. L'ordonnance d'exécution correspondante a été mise en consultation en octobre 2025. L'entrée en vigueur est prévue au deuxième semestre 2026⁶².

Enfin, le GAFI a nommé un nouveau vice-président pour la période du 1^{er} juillet 2025 au 30 juin 2027⁶³.

6.3 Taskforces

Le MROS a participé à plusieurs taskforces opérationnelles et stratégiques durant l'année sous revue, notamment le *Russia-Related Illicit Finance and Sanctions FIU Working Group* (RRIFS)⁶⁴ et la *Counter Terrorist Financing Taskforce* (CTFT)⁶⁵. Ces deux taskforce permettent d'échanger sur les risques actuels, les configurations de cas et les questions méthodologiques. Plusieurs séances ont été organisées en 2025 auxquelles le MROS était présent.

6.4 Rencontres bilatérales

Le MROS a cultivé l'échange direct avec des CRF étrangères partenaires durant l'année sous revue. Ces contacts lui ont permis de mieux comprendre les cadres juridiques respectifs et l'accès aux informations de ses partenaires. Ils favorisent un traitement efficace des dossiers et une utilisation ciblée des ressources. En outre, ils fournissent l'occasion d'un échange stratégique sur l'évolution de la criminalité organisée et du financement du terrorisme, sans oublier les questions techniques de l'échange de données.

En 2025, le MROS a mené des discussions bilatérales notamment avec les CRF des pays suivants : France, États-Unis, Nigéria, Italie, Émirats arabes unis, Qatar, Bahreïn, Autriche, Monaco, Liechtenstein et Allemagne.

La CRF allemande a organisé la réunion des CRF germanophones en décembre 2025, qui parmi les thèmes abordés, s'est notamment demandé comment gérer le volume croissant de données par rapport aux ressources disponibles. La préparation aux prochaines évaluations mutuelles des pays du GAFI était également à l'ordre du jour.

Durant l'année sous revue, le MROS a conclu des mémorandums d'entente avec les CRF de la France, du Kazakhstan, de la Chine et de l'Islande. Ces conventions définissent le cadre de l'échange d'informations et de la coopération opérationnelle.

⁶¹ GAFI, [Guidance on Beneficial Ownership and Transparency of Legal Arrangements](#) (en anglais uniquement)

⁶² [Le Conseil fédéral ouvre la consultation sur les ordonnances relatives à la transparence des personnes morales et à la lutte contre le blanchiment d'argent et le financement du terrorisme](#)

⁶³ [Résultats de la plénière du GAFI, 19-21 février 2025](#)

⁶⁴ [Russia-Related Illicit Finance and Sanctions FIU Working Group \(RRIFS Task Force\)](#) (en anglais uniquement)

⁶⁵ [Counter Terrorist Financing Taskforce \(CTFT\)](#) (en anglais uniquement). Remarque : le nom de la taskforce a depuis été modifié, passant de CTFTI à CTFT et ses activités sont désormais axées sur la lutte générale contre le financement du terrorisme.

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.

En 2025, le MROS était subdivisé en six domaines. Il employait en moyenne 66 collaborateurs, correspondant à 57 équivalents temps plein.

L'organigramme représente l'organisation actuelle du MROS et la répartition des tâches en six domaines.

Planification et affaires politiques (PuP)

Le Domaine PuP fonctionne comme une discipline transversale classique et traite tous les dossiers juridiques, politiques et stratégiques jusqu'au niveau du Conseil fédéral, notamment les projets de loi, les documents stratégiques et les interventions parlementaires. De plus, il assure la coordination et la réalisation des projets et des publications du MROS. Il garantit l'unité de doctrine et apporte son soutien aux domaines opérationnels du MROS pour les questions juridiques et conceptuelles. Il est également chargé de la gestion des risques. Enfin, 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 la réception, de l'examen formel et de l'enregistrement de toutes les communications de soupçons entrantes, y compris leur traitement du point de vue formel et technique ainsi que les corrections manuelles requises lorsque la qualité des données n'est pas satisfaisante. Par ailleurs, il prend en charge le tri des cas, les transmet à l'un des domaines opérationnels 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'assistance administrative nationale en vertu de l'art. 29 LBA.

Analyse opérationnelle Cantons (OAK)

Le Domaine OAK analyse les communications de soupçons entrantes qui relèvent pour la plupart de la compétence des autorités de poursuite pénale cantonales et qui lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées et analysées aux autorités de poursuite pénale compétentes. 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 des êtres humains et les faux dans les titres.

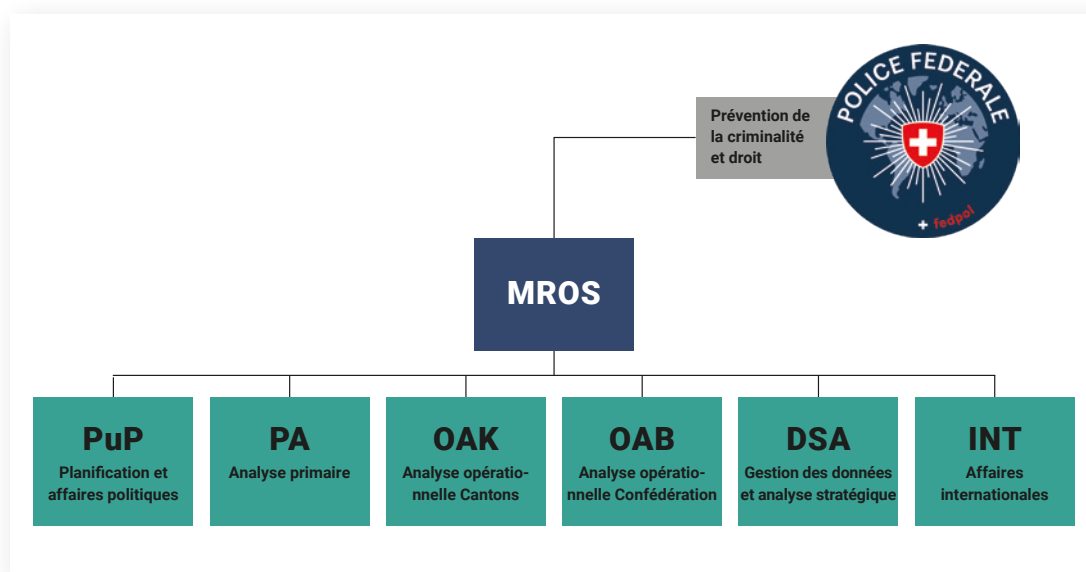


Fig. 12: Organigramme du MROS

Analyse opérationnelle Confédération (OAB)

Le Domaine OAB analyse les communications de soupçons entrantes qui relèvent a priori du MPC et qui lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées et analysées 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), la criminalité organisée, le terrorisme, les délits boursiers, l'extrémisme de droite et de gauche et 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 du système d'information du MROS (goAML) et de son développement technique. Il apporte une assistance technique aux acteurs soumis à l'obligation de communiquer, en particulier pour le raccordement et l'exploitation 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 évalue 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 est responsable de l'ensemble des échanges (d'informations) avec les CRF étrangères. Il coordonne en outre l'adhésion du MROS aux organes internationaux et sa participation aux forums de coopération multilatéraux et bilatéraux, notamment au Groupe Egmont, au GAFI, à la Convention des Nations Unies contre la corruption (CNUCC) et à l'PEFIPPP.

