



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 2023

Mai 2024

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

Rapport annuel 2023

Mai 2024

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

Téléphone: (+41) 58 463 40 40

E-mail: meldestelle-geldwaescherei@fedpol.admin.ch

Internet: www.fedpol.admin.ch

Table des matières

1.	Avant-propos	6
2.	Développements stratégiques importants	7
2.1	Volume de communications élevé – causes	7
2.2	Orientation du MROS – développement de l’approche fondée sur les risques	8
2.3	Évaluation nationale des risques – rapport sectoriel sur les cryptomonnaies et les actifs virtuels	10
2.4	Partenariat-public-privé (PPP)	12
2.5	Projet de loi sur le registre de transparence et révision de la LBA	13
2.5.1	Présentation du projet	13
2.5.2	Conséquences pour le MROS	14
2.6	Développements internationaux	14
2.6.1	Sanctions contre la Russie	14
2.6.2	Attaques terroristes du Hamas contre Israël	15
2.7	Mise en œuvre du projet Top 30 au sein du Domaine Affaires internationales	16
2.8	Crypto Symposium du MROS	17
3.	Système d’information goAML	18
4.	Statistique annuelle du MROS	20
4.1	Constatations générales 2023	20
4.2	Communications de soupçons	21
4.3	Communications de soupçons par secteur d’activité des IF	21
4.4	Bases légales des communications	22
4.5	Infractions préalables	23
4.6	Éléments à l’origine des soupçons	24
4.7	Dénonciations aux autorités de poursuite pénale	24
4.8	Retour des autorités pénales	25
4.9	Financement du terrorisme	26
4.10	Criminalité organisée	27
4.11	Communications de soupçons en rapport avec les cryptomonnaies	28
4.12	Remise d’informations au sens de l’art. 11a LBA	28
4.13	Communications de rupture de la relation d’affaires au sens de l’art. 9b LBA	29
4.14	Échange d’informations avec les homologues étrangers (CRF)	30
4.15	Échange d’informations avec les autorités suisses	30
5.	Typologies	31
5.1	Typologie 1 – coopération nationale et internationale	31
5.2	Typologie 2 – utilisation des instruments légaux	33
5.3	Typologie 3 – procédure d’analyse globale	34

6.	Pratique du MROS	37
6.1	Interprétation de l'art. 11a LBA – remise d'informations par les IF	37
6.2	Interprétation de l'article 29a LBA – annonce des jugements et des décisions par les autorités pénales	38
7.	Coopération internationale en matière de lutte contre le blanchiment d'argent	40
7.1	Groupe Egmont	40
7.2	GAFI	41
8.	Organisation du MROS	43

1. Avant-propos

Au cours de la dernière décennie, les communications de soupçons ont augmenté en moyenne de 20 à 30 % par an. Cette tendance s'est poursuivie en 2023, mais l'augmentation a été beaucoup plus forte que prévu. À la fin 2023, le MROS¹ enregistrait au total 11 876 communications de soupçons, qui correspondent à quelque 21 500 relations d'affaires et représentent une moyenne de 47 communications par jour ouvrable. Il en résulte une augmentation de 56 % par rapport à l'année précédente.

De manière générale, le volume total des rapports et des données s'est accru. En 2023, le MROS a reçu au total 21 375 rapports : communications de soupçons, réponses des intermédiaires financiers (IF) aux demandes du MROS (art. 11a LBA²), communications de rupture (art. 9b LBA), demandes internationales d'autres cellules de renseignements financiers (CRF) et informations spontanées d'autorités nationales et internationales (cf. ch. 4). La communication avec les IF passe presque exclusivement par l'application informatique goAML (*government office Anti-Money Laundering*). Les IF transmettent majoritairement les données de manière structurée. Cette évolution est réjouissante. Cependant, il y a encore un potentiel d'amélioration du côté des autorités dont la part de données non structurées reste très élevée et représente actuellement près de 30 % du volume total (cf. ch. 3).

En 2023, le MROS a transmis au total 866 dénonciations aux autorités de poursuite pénale. Cette baisse de près de 30 % par rapport à l'année précédente résulte notamment de la stratégie du MROS consistant à agir en fonction des risques et à se concentrer sur la grande criminalité. Les analyses réalisées par le MROS dans ce domaine sont plus approfondies et plus complexes. Ainsi, le MROS a, en 2023, transmis 43 % de dénonciations supplémentaires au Ministère public de la Confédération (MPC) par rapport à l'année précédente ; les cantons ont par contre été moins saisi, à l'exception du Ministère public de Genève. En outre, les transmissions pour escroquerie au prêt COVID ont totalement disparu en 2023. Par ailleurs, les dénonciations aux autorités de poursuite pénale regroupent de plus en plus de communications de soupçons différentes – le nombre de transmissions est donc moindre et une comparaison avec les années précédentes n'est que partiellement pertinente (cf. ch. 2.2).

Berne, mai 2023

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

¹ Money Laundering Reporting Office Switzerland

² Loi du 10 octobre 1997 sur le blanchiment d'argent (LBA ; RS 955.0)

2. Développements stratégiques importants

2.1 Volume de communications élevé – causes

Au cours de la dernière décennie, les communications de soupçons ont augmenté en moyenne de 20 à 30 % par an. Cette hausse s'explique de plusieurs manières. Elle est due pour l'essentiel au renforcement continu, depuis 2013, des exigences réglementaires en matière d'obligations de diligence et de communication. La surveillance des marchés financiers et l'application du droit se sont ainsi considérablement renforcées. Les nombreux scandales de corruption et de blanchiment d'argent qui ont impliqué une grande partie du secteur bancaire suisse ont rendu les IF encore plus conscients de l'importance de lutter efficacement contre le blanchiment d'argent. De nombreuses banques ont renforcé les effectifs des services chargés de la conformité et de la criminalité financière. En outre, elles ont pu affiner en permanence la surveillance des transactions grâce aux progrès technologiques. Le passage du système de communication en papier à l'application informatique goAML et la connexion XML³ au 1^{er} janvier 2020 ont simplifié la communication des déclarations de soupçons pour le secteur financier. Tous ces développements entraînent une augmentation des communications de soupçons faites au MROS. Cette tendance s'est poursuivie en 2023, mais l'augmentation a été beaucoup plus forte que

prévu. À la fin de l'année en question, le MROS avait enregistré un total de 11 876 communications, soit une hausse de plus de 4 200 communications ou de 56 %. Les communications ont doublé en l'espace de deux ans et même décuplé sur les dix dernières années. Ce volume impressionnant appelle une mise en perspective et doit faire l'objet de prévisions pour les années à venir, tant ses répercussions sont importantes pour le MROS et son orientation stratégique.

La nette hausse du volume de communications est due, pour le MROS, aux facteurs suivants :

- **Inscription de la définition des soupçons fondés dans la loi :** le projet du Secrétariat d'État aux questions financières internationales (SFI)⁴ est entré en vigueur le 1^{er} janvier 2023. La notion de soupçons fondés, déjà établie par la pratique et la jurisprudence depuis plus de dix ans, est désormais inscrite dans la loi (art. 9, al. 1^{quater}, LBA). Elle implique qu'un IF doit toujours faire une communication de soupçons lorsqu'il dispose d'un signe concret ou de plusieurs indices laissant supposer que des valeurs patrimoniales pourraient être d'origine criminelle et que les clarifications supplémentaires effectuées ne permettent pas de dissiper les soupçons. Une partie des communications est probablement due à cette formulation désormais sans équivoque de la loi.

³ Le schéma XML évoqué ici définit la structure des informations fournies au MROS par les IF au moyen d'un fichier au format XSD. D'autres informations se trouvent sur le site Internet du MROS. Cf. Informations concernant le système de traitement des données goAML au MROS (admin.ch).

⁴ RO 2021 656; cf. aussi le message du 26 juin 2019 concernant la modification de la loi sur le blanchiment d'argent, FF 2019 5237, pp. 5250 ss.

- **Durcissement de la pratique en ce qui concerne l'art. 37 LBA**: les sanctions pénales prévues en cas de violation de l'obligation de communiquer ont été renforcées. Une analyse des jugements rendus par le Département fédéral des finances (DFF) et le Tribunal pénal fédéral montre que de plus en plus de responsables de la conformité issus des échelons hiérarchiques inférieurs sont désormais appelés à rendre des comptes⁵. Les condamnations pour violation par négligence de l'obligation de communiquer ont également augmenté⁶. Des entretiens menés avec des représentants du secteur de la finance ont montré que ce durcissement de la pratique a eu un effet sur eux et influence par conséquent leur comportement. Ces derniers préfèrent communiquer trop plutôt qu'insuffisamment.
- **Sociétés d'audit et organes de révision (internes) aux exigences élevées**: les retours d'information des IF indiquent que les sociétés d'audit, de même que les organes de révision internes, ont tendance à apprécier plus sévèrement le respect des exigences prudentielles en matière de blanchiment d'argent. Le renforcement général du dispositif de surveillance et de lutte contre le blanchiment d'argent ainsi que la plus grande focalisation des médias sur le secteur de l'audit pourraient en être la cause.
- **Pression des coûts sur les IF ayant un modèle d'affaires asymétrique**: la pression des coûts sur le secteur de la finance est palpable. Les faits ne sont parfois plus clarifiés que de manière très rudimentaire et les obligations particulières en la matière au sens de l'art. 6 LBA, qui s'appliquent en cas de communication de soupçons au MROS, ne sont plus remplies, ou alors le sont de manière insuffisante. Ce phénomène est particulièrement visible dans les établissements financiers ne faisant pas de gestion de fortune, qui démarchent agressivement les

clients étrangers. Une grande partie de ces communications de soupçons insuffisamment clarifiées n'ont aucune valeur pour le MROS. En adoptant un tel comportement, les IF ne remplissent plus, ou alors seulement insuffisamment, leur fonction de première ligne de défense dans le dispositif de lutte contre le blanchiment d'argent. Le MROS et la FINMA se concertent sur les IF concernés et les mesures engagées.

On peut s'attendre que la forte hausse tendancielle des communications se poursuive en 2024 et au-delà. L'expérience montre que de telles évolutions sont généralement irréversibles. Une fois que le comportement décrit en matière de communication s'est établi, il devient la norme. Il est peu probable que le secteur de la finance fasse marche arrière de sa propre initiative, d'autant moins que les signaux envoyés par les autorités pénales et les autorités de surveillance, mais aussi par le Groupe d'action financière sur le blanchiment de capitaux (GAFI), laissent plutôt présager un durcissement. Il faudra donc s'attendre à une augmentation des communications à l'avenir. Le MROS n'est que partiellement équipé pour faire face à une nouvelle augmentation du volume des communication similaire à 2023. Ses effectifs et ses ressources techniques atteignent leurs limites. L'application de l'approche fondée sur les risques (cf. ch. 2.2) permet certes de gérer cette hausse en renforçant les critères de prise en charge (soit de tri), mais dans les faits, la décision d'analyser de manière approfondie une communication de soupçons ne dépendrait alors plus du risque, mais des ressources.

2.2 Orientation du MROS – développement de l'approche fondée sur les risques

La méthode de travail du MROS a beaucoup évolué ces dernières années. En raison de l'augmentation massive des communications de soupçons et du volume des rapports, le MROS

⁵ Entre 2014 et 2022, le DFF et le Tribunal pénal fédéral ont prononcé au moins 21 condamnations entrées en force. À la fin de 2022, 47 procédures étaient en cours (source: Strafrechtliche Verantwortlichkeit des Compliance Officers, exposé de Doris Hutzler du 8 juin 2023 à l'occasion de la 14e Journée du droit pénal économique de l'Europa Institut an der Universität Zürich).

⁶ Cf. par ex. l'arrêt 6B_1176/2022 du Tribunal fédéral du 5 décembre 2023.

n'est plus en mesure d'analyser et de traiter toutes les informations avec le même degré de précision qu'il y a cinq ou dix ans. Il se voit contraint de fixer des priorités et des objectifs principaux. Depuis qu'il a introduit goAML le 1^{er} janvier 2020, il a adopté une approche fondée sur les risques pour la réception et le traitement des communications de soupçons: les communications entrantes sont catégorisées en fonction du risque à l'aide d'une matrice de tri, classées par ordre de priorité, puis analysées selon différents critères sur la base de ce classement. Le MROS se concentre sur la lutte contre la grande criminalité, en mettant l'accent sur la criminalité organisée, le financement du terrorisme ainsi que certaines formes de criminalité économique. Pour ce faire, il s'oriente également en fonction des stratégies des autorités de poursuite pénale, il cherche à obtenir les meilleurs résultats possibles, tout en tenant compte des risques de réputation potentiels pour la place financière suisse.

La stratégie du MROS se reflète aussi dans les statistiques actuelles. Alors que les dénonciations au MPC ont augmenté en 2023 (+43% par rapport à 2022)⁷, celles faites aux autorités de poursuite pénale cantonales sont en recul par rapport aux années précédentes, à l'exception du canton de Genève. Cette situation s'explique par le fait que les dénonciations effectuées par le MROS ont été plus nombreuses dans le domaine de la grande criminalité. En 2023, le MROS en a transmis au total 866 aux autorités de poursuite pénale. À titre de comparaison, il y en avait eu 1232 en 2022 et 1486 en 2021⁸. S'il s'agit d'une baisse quantitative, les informations que contiennent les dénonciations montrent toutefois que celles-ci comptaient davantage de communications de soupçons et de réponses des IF par transmission en 2023. En 2021, une dénonciation aux autorités de poursuite pénale contenait en moyenne 1,3 communication de soupçons; en 2023, ce chiffre était de 1,8. En

outre, en 2023, des informations supplémentaires fournies par les IF ont été traitées dans 44% des affaires complexes transmises aux autorités de poursuite pénale, contre 18% en 2021 et 25% en 2022. Ces chiffres démontrent que les analyses actuelles du MROS ont tendance à contenir plus d'informations et à être plus complexes. Le MROS s'éloigne ainsi de l'approche de traitement traditionnelle *1 communication = 1 dénonciation aux autorités de poursuite pénale* pour s'orienter vers un renseignement actif et vers la mise en réseau des informations disponibles. Ce n'est plus la communication de soupçons en tant que telle qui est au centre de l'analyse, mais son contenu informatif.

Ces prochaines années, le MROS va continuer de développer systématiquement sa stratégie de renseignement: focalisation, tri, priorisation, mise en réseau. Force est toutefois de constater que la part des communications de soupçons pouvant faire l'objet d'une analyse approfondie baisse constamment en raison de l'augmentation continue du volume de rapports⁹. En 2023, une communication sur cinq a été analysée en profondeur¹⁰. Les 80% de communications restantes ont été traitées de manière moins intensive ou à l'aide de méthodes d'analyse globales, comme les méthodes d'agrégation (*clustering*). Une partie des communications ont déjà été triées au moment de la réception. Cela signifie que ces communications et les informations qu'elles contiennent ne font plus l'objet d'un suivi ultérieur. Elles peuvent toutefois être réactivées et traitées à tout moment puisqu'elles sont préparées et enregistrées dans goAML. En 2023, plus de 300 (anciennes) communications de soupçons triées ont été réactivées en raison d'une nouvelle information, par exemple la communication de soupçons d'un IF ou l'information spontanée d'une CRF étrangère. L'augmentation des communications de soupçons accroît le risque que des cas importants de blanchiment d'argent ne soient pas identifiés.

⁷ Transmissions au MPC: 79 en 2022, 113 en 2023

⁸ Cf. à ce sujet le ch. 4.7: les statistiques des années 2021 et 2022 comprennent aussi les transmissions dites COVID, ce qui les pousse à la hausse.

⁹ Les communications de soupçons ont augmenté de 56% en 2023 et le volume total de rapports de 63%.

¹⁰ Analyses approfondies: 45% en 2021, 32% en 2022

Le MROS s'efforce d'augmenter sa cadence de traitement et son efficacité. Les facteurs limitant la réception et le tri des communications de soupçons sont, outre les effectifs, le soutien technique (automatisation, soutien informatique intelligent), la qualité des données des communications entrantes et les informations fournies par les IF. Ces derniers ont un effet déterminant sur l'efficacité du traitement des données. Plus la qualité des données est mauvaise, plus le processus de traitement est laborieux. Pour combler ces lacunes, il faudrait un meilleur soutien informatique ou des effectifs supplémentaires. En 2023, le MROS a continué à faire avancer le projet informatique goAML Futuro¹¹, qui vise à assurer une interopérabilité, soit la comparaison automatique des bases de données judiciaires et policières accessibles. Le MROS a également obtenu des améliorations en ce qui concerne la discontinuité des données. C'est en effet la qualité des données lors de la réception des communications qui lui pose le plus de difficultés et recèle donc aussi le plus grand potentiel d'amélioration de l'efficacité. L'introduction prévue de l'art. 23, al. 7, LBA dans le cadre de la révision en cours de la loi¹² est d'une importance capitale pour le MROS. fedpol serait ainsi habilité à prescrire par voie d'ordonnance technique sous quelle forme et dans quel format (norme concernant les données) les données devraient être livrées.

2.3 Évaluation nationale des risques – rapport sectoriel sur les cryptomonnaies et les actifs virtuels

Les risques liés au blanchiment d'argent et au financement du terrorisme devraient toujours faire partie de la stratégie de lutte contre la criminalité d'un pays. La Suisse a publié à ce jour deux

évaluations nationales des risques (*national risk assessment*), en juin 2015¹³ et en octobre 2021¹⁴. Les risques existants, y compris les risques sectoriels qui les sous-tendent, y sont analysés dans le détail sur mandat et sous la responsabilité du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF)¹⁵. Le MROS fait partie de ce groupe et, en tant que responsable du sous-groupe analyse des risques, est chargé d'élaborer les rapports sur les risques.

Le rapport sectoriel relatif au risque de blanchiment d'argent et de financement du terrorisme par les crypto-actifs, élaboré sous la direction du MROS, a été adopté par le GCBF le 5 décembre 2023¹⁶. Un premier rapport relatif au risque de blanchiment d'argent et de financement du terrorisme par les crypto-actifs et le financement participatif, publié en octobre 2018¹⁷, qualifiait d'importantes les menaces et les vulnérabilités concernant la Suisse. L'influence et l'importance des actifs virtuels (AV) ont radicalement changé depuis 2018. Le marché y a été nettement sensibilisé et sa prise de conscience s'est notablement accrue. Depuis lors, le MROS reçoit tous les jours des communications de soupçons en rapport avec des AV, qui font désormais partie du quotidien des autorités de poursuite pénale. Il a constaté quatre évolutions principales :

1. Le nombre d'IF exerçant en Suisse une activité de prestataire de services d'actifs virtuels (PSAV) a nettement augmenté, passant de moins de dix en 2018 à plus de 204 à la fin de 2022. Malgré cela, au moins 180 de ces IF n'ont pas envoyé de communications de soupçons au MROS.
2. L'utilisation des AV s'est multipliée en Suisse entre 2018 et 2023. De plus en plus de par-

¹¹ Cf. les explications dans le *Rapport annuel 2022 du MROS*, p. 13 s.

¹² *Communiqué de presse du Conseil fédéral du 30 août 2023* : Le Conseil fédéral met en consultation un projet de loi visant à améliorer la lutte contre le blanchiment d'argent.

¹³ *Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, Juin 2015*.

¹⁴ *Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse*, Octobre 2021.

¹⁵ Le GCBF est dirigé par le Secrétariat d'État aux questions financières internationales (SFI), dont le mandat est décrit *ici*.

¹⁶ *National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets* (en allemand uniquement).

¹⁷ *Rapport Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding, Octobre 2018*.

ticuliers et d'entreprises les utilisent et les acceptent pour des transactions commerciales, des services et des investissements. La frontière entre le secteur financier traditionnel et le domaine des AV devient de plus en plus floue; les AV sont de plus en plus intégrés dans les plates-formes de paiement conventionnelles, d'où la fusion de ces deux mondes.

3. L'utilisation des AV à des fins criminelles a augmenté, tant en Suisse que dans le monde. Elle s'est en outre considérablement diversifiée. Les autorités de poursuite pénale sont de plus en plus souvent confrontées à des procédures liées à différents secteurs économiques qui présentent des liens avec les AV. Par exemple, de plus en plus de dénonciations sont faites lorsque des AV sont volés ou détournés d'une autre manière, notamment par escroquerie ou gestion déloyale. Les montants des dommages ainsi causés ont fortement augmenté et s'élèvent en Suisse à plusieurs dizaines de millions de francs au moins pour 2022; à titre de comparaison, ils atteignaient juste 7 millions en 2007. L'utilisation de AV s'est généralisée pour certaines infractions commises par des moyens comme la fraude à l'investissement et les rançongiciels. Ils sont devenus un outil courant de la criminalité financière.
4. Ces dernières années, les IF en Suisse ont constaté, sur les comptes qu'ils gèrent, que le recours à des AV était de plus en plus fréquent dans des opérations relevant probablement du blanchiment d'argent et du financement du terrorisme. Il en résulte une forte hausse des communications de soupçons relatives aux AV: en 2022, près de 14% de toutes ces communications présentaient déjà un lien avec des AV. Ces dernières ont notamment mis en lumière des liens avec des personnes politiquement exposées, des affaires de corruption internationales, des groupes transnationaux impliqués dans la criminalité organisée ou des acteurs étatiques.

L'évaluation des risques conclut que les risques de blanchiment d'argent et de financement du terrorisme liés aux AV ont augmenté depuis 2018.

Les menaces et les vulnérabilités qui avaient déjà été identifiées alors se sont pour la plupart aggravées et étendues. En raison de leur importance accrue et des risques qu'ils comportent, les AV requièrent l'attention de tous les partenaires concernés (IF, CRF, autorités de poursuite pénale, autorités de surveillance et organismes de surveillance et d'autorégulation).

Malgré les menaces et les vulnérabilités identifiées auxquelles la Suisse se retrouve exposée en matière de blanchiment d'argent et de financement du terrorisme liés aux AV, différents facteurs contribuent à réduire ces risques:

- Lors d'enquêtes sur les AV, la coopération internationale montre que le renforcement du suivi, le blocage et la confiscation des AV permettent de lutter efficacement contre le blanchiment d'argent et le financement du terrorisme.
- De nombreux petits fournisseurs de AV ont aujourd'hui disparu ou ont fusionné. Dès lors, les grandes cryptobourses ont renforcé leurs mesures de conformité, ce qui consolide le dispositif de défense au niveau mondial.
- Les blockchains sont par nature plus transparentes que les systèmes de paiement traditionnels, d'où une meilleure traçabilité des AV. Les outils d'analyse de la blockchain peuvent plus facilement identifier et suivre les activités suspectes.
- Enfin, l'élargissement de la définition de l'intermédiation financière dans le domaine des AV contribue en Suisse à faire entrer un plus large éventail d'acteurs dans le champ d'application de la LBA. Cet élargissement permet de combler des lacunes dans les mesures de lutte contre le blanchiment d'argent et le financement du terrorisme.

Sur la base des conclusions du rapport, le GCBF propose quatre mesures visant à renforcer le dispositif actuel de défense contre le blanchiment d'argent et le financement du terrorisme dans le domaine des AV:

- 1. Améliorer l'état des données et des connaissances sur le secteur des AV en Suisse**
les informations sur le secteur des AV et sur leur utilisation criminelle en Suisse sont indis-

pensables pour identifier, comprendre et évaluer correctement les risques de blanchiment d'argent et de financement du terrorisme.

2. Encourager un comportement proactif en matière de communication de la part des IF exerçant une activité de PSAV

les IF exerçant une activité de PSAV devraient à l'avenir renforcer leurs investigations en matière de blanchiment d'argent et de financement du terrorisme afin d'être mieux à même de détecter les opérations suspectes et de les communiquer au MROS.

3. Fournir des effectifs et des ressources suffisants pour lutter contre le blanchiment d'argent et le financement du terrorisme dans le domaine des AV

la coopération entre toutes les parties prenantes concernées doit être renforcée afin de résoudre les difficultés que présente la lutte contre le blanchiment d'argent et le financement du terrorisme dans le domaine des AV.

4. Renforcer la coopération internationale

la Suisse doit continuer à s'engager au niveau international pour combattre efficacement les risques de criminalité propres au secteur financier et faire progresser la mise en œuvre de la recommandation du GAFI.

En conclusion, le rapport sectoriel souligne que la Suisse doit prendre au sérieux les risques liés aux AV et adopter des mesures appropriées pour combattre efficacement les deux phénomènes précités. L'importance des AV dans le secteur financier ne cessant de croître, la Suisse doit prendre les problèmes à bras-le-corps pour rester en phase avec ces développements rapides. Le rapport sectoriel précité relatif au risque de blanchiment d'argent et de financement du terrorisme par les crypto-actifs a été publié au premier trimestre de 2024¹⁸. Des rapports sectoriels supplémentaires sont en cours de planification sous l'égide du MROS: *Financement de la prolifération* (parution prévue au troisième trimestre de 2024), *Personnes morales* (parution prévue au

quatrième trimestre de 2024) et *Marché immobilier* (parution prévue dans le courant de 2025).

2.4 Partenariat-public-privé (PPP)

Le 17 novembre 2021, le Conseil fédéral a chargé fedpol, plus précisément le MROS, d'examiner en collaboration avec d'autres autorités les possibilités d'instaurer un PPP destiné à l'échange d'informations financières, dans le but de renforcer encore la lutte contre le blanchiment d'argent et le financement du terrorisme en Suisse. Le MROS a mené en 2022 des discussions approfondies sur l'utilité et les conditions-cadres d'un PPP avec le SFI, le Département fédéral des affaires étrangères, l'Autorité fédérale de surveillance des marchés financiers (FINMA) et un groupe d'experts composé de représentants de la finance. Les autorités et les experts ont conclu qu'un PPP pourrait apporter une contribution significative à la lutte contre la criminalité, notamment en renforçant la prévention. Le MROS a rédigé un rapport¹⁹ sur les principaux résultats de l'échange entre autorités et experts et l'a soumis au Conseil fédéral en avril 2023 pour qu'il en prenne connaissance. Un groupe de travail composé du MROS, du SFI et de représentants de différents secteurs de la finance a été mis sur pied à cet effet. Les travaux de création d'un PPP en Suisse sont toujours en cours. D'ici à la fin 2024 au plus tard, toutes les questions en suspens devront être résolues et un échange durable entre les secteurs public et privé devra avoir eu lieu sur la base de règles à définir.

Le MROS participe aujourd'hui déjà à un PPP, qui a pour nom Europol Financial Intelligence Public Private Partnership (EFIPPP)²⁰. L'EFIPPP a été lancé en 2017 par le Centre européen de lutte contre la criminalité financière et économique, rattaché à Europol. Il vise à promouvoir la coopération transfrontalière et l'échange d'informations entre Europol, les autorités de poursuite pénale, les CRF, les organismes de surveillance ainsi que les prestataires de services financiers réglementés.

¹⁸ *National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets* (en allemand uniquement)

¹⁹ *Partenariat-public-privé (PPP) relatif à l'échange d'informations dans la lutte contre le blanchiment d'argent et le financement du terrorisme*, mars 2023

²⁰ *Page d'accueil de l'EFIPPP*

L'EFIPPP est la première plate-forme d'échange d'informations transnationale. Lors de son lancement, il était composé de 28 institutions publiques ou privées issues de huit États membres ou non membres de l'Union européenne (UE). Au début de 2022, il comprenait 79 institutions issues de 18 États membres ou non membres de l'UE.

L'EFIPPP poursuit les objectifs suivants :

- développer ensemble un socle d'informations et une compréhension commune ;
- élaborer en commun des indicateurs de risques et des typologies de menaces ;
- faciliter l'échange de renseignements opérationnels ou tactiques dans le cadre d'enquêtes en cours, conformément aux dispositions juridiques nationales et internationales en vigueur ;
- identifier les passerelles d'échange d'informations et les obstacles juridiques à l'échange d'informations, conformément aux cadres juridiques nationaux et européen en vigueur ;
- promouvoir l'utilisation de nouveaux outils de lutte contre la criminalité financière, l'utilisation de nouvelles technologies et l'échange d'expériences et de méthodes communes à des fins d'innovation et de formation ;
- soutenir les forums de coopération nationaux au sein des juridictions concernées, dans le but de servir de plaque tournante efficace entre les différentes plates-formes et de faciliter l'échange d'informations et de renseignements au titre du PPP.

La structure de l'EFIPPP repose sur quatre piliers :

- **Strategic Oversight Body** : l'organe de surveillance stratégique est responsable des conseils stratégiques et de la coordination concernant les questions liées au développement et aux domaines prioritaires de l'EFIPPP. Il se réunit tous les ans ;
- **Steering Group** : le groupe de pilotage dirige les activités opérationnelles de l'EFIPPP et fait office d'organe de décision. Il définit les priorités de chaque année civile, approuve l'admission de nouveaux membres et régleme-nte les activités des groupes de travail ;

- **Working Groups** : différents groupes de travail, actuellement au nombre de sept, réalisent les objectifs de l'EFIPPP et mettent au point ses différents produits et documents. Ils constituent son cœur opérationnel ;
- **Threat and Typologies Group** : ce groupe s'occupe principalement de constituer des connaissances sur certaines menaces.

Le MROS profite dans une large mesure des informations échangées au sein de l'EFIPPP. Le courrier de sensibilisation, dénommé alerte, que le MROS a envoyé le 3 novembre 2023 au secteur financier suisse concernant le financement du terrorisme ainsi que l'addendum du 5 décembre 2023 reposent en grande partie sur des informations et des analyses provenant de l'EFIPPP. Un échange d'informations international fluide est aujourd'hui la clé d'une lutte efficace et crédible contre le blanchiment d'argent. Le MROS participe activement à l'EFIPPP et est membre du groupe de pilotage depuis décembre 2023.

2.5 Projet de loi sur le registre de transparence et révision de la LBA

2.5.1 Présentation du projet

Lors de sa séance du 12 octobre 2022, le Conseil fédéral a chargé le DFF d'élaborer un projet de loi visant à accroître la transparence et à faciliter l'identification des ayants droit économiques des personnes morales. Ce projet vise à renforcer l'intégrité de la place financière et économique suisse. Il prévoit l'introduction d'un registre fédéral des ayants droit économiques (registre de transparence) ainsi que d'autres mesures nécessaires pour accroître l'efficacité du dispositif de lutte contre le blanchiment d'argent et la criminalité économique. Ces mesures permettent de s'adapter à l'évolution des normes internationales (GAFI et Forum mondial) et de garantir que la Suisse s'y conforme. Le projet comprend les points suivants :

- la création d'un **registre fédéral de transparence** des ayants droit économiques d'entités juridiques. Ce registre, qui ne sera pas accessible au public, sera géré par le DFJP. L'organe de contrôle, rattaché au DFF, en garantira la

- vérification qualitative et disposera d'instruments de sanction appropriés;
- l'introduction d'**obligations de diligence** au sens de la LBA pour les **activités de conseil présentant des risques** particuliers (assujettissement des conseillers et des avocats);
 - des **mesures** supplémentaires pour le commerce immobilier ainsi que celui des métaux précieux et des pierres précieuses. Enfin, le projet vise à clarifier les obligations des IF en matière de surveillance de la mise en œuvre des mesures de contrainte au titre de la loi sur les embargos²¹.

2.5.2 Conséquences pour le MROS

Le projet de loi prévoit que les IF signalent au registre toute divergence constatée entre les informations dont ils disposent et celles figurant dans le registre, du moment que ces divergences éveillent des doutes quant à l'exactitude, l'exhaustivité ou l'actualité des informations relatives à l'ayant droit économique d'une entité juridique (discrepancy reporting). Le MROS est à son tour tenu d'informer le registre si, sur la base de ses analyses, il a des doutes sur les informations que contient le registre sur l'ayant droit économique²². L'échange d'informations entre les autorités préposées au registre et le MROS se fait conformément aux dispositions d'entraide administrative adaptées que prévoit la LBA²³. L'assujettissement à la LBA des activités de conseil à risque déclenche un nouvel ensemble de communications pour le MROS, notamment – mais pas uniquement – du fait de la création et de la structuration de personnes morales, ce qui augmentera encore le volume des communications. Les adaptations supplémentaires apportées à la LBA, notamment dans le domaine du commerce immobilier ainsi que dans celui des métaux précieux et des pierres précieuses, comblent des lacunes importantes et contri-

buent à renforcer encore le dispositif de défense de la Suisse.

Le MROS soutient et salue le projet de loi sur le registre de transparence et la révision de la LBA, notamment parce que leur mise en œuvre sera également déterminante pour l'évaluation mutuelle réalisée par le GAFI. Obtenir un bon résultat à cette évaluation est d'une grande importance stratégique pour la Suisse en tant que place économique et financière internationale.

2.6 Développements internationaux

2.6.1 Sanctions contre la Russie

Les sanctions adoptées par suite de l'agression militaire de la Russie contre l'Ukraine et de la décision qu'a prise le Conseil fédéral le 28 février 2022 de reprendre les sanctions de l'UE contre la Russie²⁴ ont aussi occupé le MROS en 2023. Dans son dernier rapport annuel, ce dernier a précisé qu'il fallait faire une distinction entre les différents systèmes de communication et les compétences: les sanctions incombent au Secrétariat d'État à l'économie (SECO), alors que le blanchiment d'argent est du ressort du MROS.

La surveillance de l'exécution de l'obligation de communiquer et du respect du régime de sanctions revient au SECO. Une déclaration faite à ce dernier n'entraîne pas nécessairement une communication au MROS. Elle ne libère toutefois pas les IF des obligations de communiquer et de diligence prévues par la LBA. Si des clarifications menées par l'IF en lien avec la violation ou le contournement de sanctions font apparaître des indices de blanchiment d'argent, l'IF doit procéder à des clarifications supplémentaires (art. 6 LBA) et, en fonction des résultats, transmettre une communication au MROS²⁵. Pour effectuer une communication, l'IF doit toujours s'assurer que la condition suivante est remplie, à savoir que les valeurs patrimoniales impliquées dans

²¹ Loi du 22 mars 2002 sur les embargos (LEmb; RS **946.231**)

²² L'avant-projet de loi sur la transparence des personnes morales.

²³ Nouvel art. 29, al. 1, LBA

²⁴ *Règlement (UE) n° 833/2014* du Conseil du 31 juillet 2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine.

²⁵ Droit de communication (art. 305^{ter}, al. 2, du code pénal [CP]; RS **311.0**) ou obligation de communiquer (art. 9 LBA).

la relation d'affaires ont un rapport présumé avec le soutien d'une organisation criminelle ou terroriste ou avec le blanchiment d'argent, proviennent d'un crime ou d'un délit fiscal qualifié, sont soumises au pouvoir de disposition d'une organisation criminelle ou terroriste ou servent au financement du terrorisme. L'art. 10, al. 2, CP qualifie de crimes les infractions passibles d'une peine privative de liberté de plus de trois ans. Une violation ou le contournement de sanctions ne constituent un crime que dans des cas graves, une violation simple des sanctions n'étant pas constitutive d'une infraction préalable au sens de la LBA²⁶.

Comme en 2022, le MROS n'a pas constaté, durant l'année sous revue, de changement significatif de comportement du côté des IF par suite des sanctions prononcées. Il a certes reçu des communications relatives à des violations et à des contournements de sanctions, mais la majorité de ces communications étaient également liées à des cas présumés de blanchiment d'argent, de criminalité organisée ou de financement du terrorisme. Il voit se confirmer encore l'impression que les IF savent très bien distinguer les différents systèmes de communication et les différentes compétences et qu'ils envoient leurs communications de soupçons de manière différenciée.

Dans le cadre des échanges internationaux avec des autorités partenaires, le MROS a également répondu régulièrement à des demandes d'informations et transmis des informations spontanées en 2023 en lien avec les mesures de sanction. Dans la mesure où les conditions légales étaient remplies, il a répondu aux demandes d'entraide administrative reçues de CRF étrangères ou les a portées à la connaissance de l'autorité nationale compétente à ce titre.

Au début de 2022, le MROS a rejoint le Russia-Related Illicit Finance and Sanctions FIU Working Group (**RRIFS**)²⁷. Il s'agit d'un groupe de travail réunissant des CRF, dont celle de la Suisse.

²⁶ Art. 9, al. 1 et 2, LEmb.

²⁷ *RRIFS Task Force*.

²⁸ *CTFTI Task Force*.

²⁹ Communiqué de presse du Conseil fédéral du 21 février 2024: *Le Conseil fédéral met en consultation le projet de loi interdisant le Hamas*

³⁰ Art. 9 LBA en relation avec l'art. 260^{ter} CP

L'échange international d'informations, qui est à la fois une tâche centrale du MROS et une nécessité, se fait sur la base des dispositions de la LBA et des principes du Groupe Egmont.

2.6.2 Attaques terroristes du Hamas contre Israël

Outre l'agression militaire de la Russie contre l'Ukraine, un autre sujet international a occupé le MROS: les attaques terroristes du Hamas contre Israël. Dans ce contexte, le MROS a rejoint la Counter Terrorist Financing Taskforce – Israel (CTFTI)²⁸, sur la même base juridique que pour le RRIFS. Contrairement à ce qu'elle a fait lors de l'agression militaire de la Russie contre l'Ukraine, la Suisse n'a pas adopté de sanctions contre le Hamas. Le Conseil fédéral a décidé le 11 octobre 2023 d'interdire le Hamas en Suisse. Le 22 novembre 2023, il a chargé le DFJP et le Département fédéral de la défense, de la protection de la population et des sports d'élaborer, d'ici à la fin de février 2024, le projet de consultation relatif à une loi spéciale à cet effet, dite loi interdisant le Hamas). Le 21 février 2024, le Conseil fédéral a décidé d'ouvrir la procédure de consultation, qui court jusqu'au 28 mai 2024. L'entrée en vigueur de la loi prendra toutefois encore un certain temps²⁹.

Un IF est déjà soumis aujourd'hui à une obligation de communiquer s'il a des raisons de soupçonner que des flux financiers sont liés à une organisation terroriste ou servent à la financer ou à la soutenir³⁰. Dans la pratique, les clarifications dans ce domaine soulèvent toutefois de grandes difficultés. Tant que le Hamas n'a pas été clairement qualifié d'organisation terroriste ou interdit, il peut, par exemple, recevoir un paiement sans que cette opération justifie à elle seule une communication de soupçons au sens de la LBA en rapport avec le soutien d'une organisation terroriste au sens de l'art. 260^{ter} CP, car il doit exister en outre un soupçon selon lequel les fonds en

question sont susceptibles de servir au terrorisme ou d'être liés à un crime ou à un délit fiscal qualifié. La situation serait donc plus claire si le Hamas était qualifié d'organisation terroriste et interdit en vertu de la loi ad hoc, de sorte qu'une simple transaction suffirait à générer un soupçon suffisant d'infraction préalable au blanchiment d'argent.

2.7 Mise en œuvre du projet Top 30 au sein du Domaine Affaires internationales

La coopération internationale est une pierre angulaire de l'activité du MROS. Le blanchiment d'argent est un phénomène mondial qui se joue des frontières nationales. De nombreuses informations qu'analyse le MROS contiennent des informations provenant d'homologues étrangers (les CRF). À leur tour, ces derniers demandent de plus en plus d'informations au MROS concernant des relations d'affaires ouvertes auprès d'IF suisses. Les échanges se sont intensifiés au cours des dernières années. Or, les demandes d'entraide administrative qui sont adressées aux autorités partenaires étrangères ou qui en proviennent n'augmentent pas seulement quantitativement, mais aussi au niveau de leur contenu, qui s'est enrichi. L'une des principales raisons de cette évolution est que le MROS s'est vu octroyer en 2021 la compétence élargie de procéder à des clarifications auprès des IF sur mandat de CRF étrangères (art. 11a, al. 2^{bis}, LBA). Les CRF étrangères ont ainsi compris, depuis la modification de la loi en Suisse, qu'elles pouvaient obtenir des informations auprès des IF suisses par l'intermédiaire du MROS même en l'absence de communications de soupçons. L'échange transnational est soumis à des exigences strictes, mais il est très utilisé. Afin d'améliorer la coopération internationale, de simplifier les procédures et d'augmenter l'efficacité de l'échange d'informations, il est important que le MROS connaisse les besoins et les spécificités de ses homologues. C'est pourquoi il a lancé le projet Top 30 en 2023. Ce projet répondait à une recommandation formulée par le Contrôle fédéral des finances (CDF) dans son audit du 20 décembre

2021 sur la réalisation des tâches du MROS³¹. Il avait pour objectif d'analyser les informations que recevait le MROS, les réponses qu'il fournissait aux CRF étrangères et d'identifier les schémas, les anomalies et les points faibles propres à cette coopération. Les données ont été évaluées pour la période allant du 1^{er} juillet 2021 (entrée en vigueur de l'art. 11a, al. 2^{bis}, LBA) au 30 juin 2022.

Sans surprise, il s'est avéré que huit des dix CRF ayant adressé le plus de demandes au MROS étaient des CRF européennes. En outre, le classement du Top 30 comprenait notamment les CRF disposant elles-mêmes d'une grande place financière ou ayant d'autres liens (économiques) étroits avec la place financière suisse. Il englobait aussi des juridictions renommées, attrayantes pour l'établissement de sociétés de domicile., ainsi que les informations spontanées reçues de l'étranger et les demandes que le MROS lui avait adressées.

La coopération a été évaluée d'un point de vue tant qualitatif que quantitatif. Par ailleurs, les CRF étrangères ont été interrogées sur leur degré de satisfaction quant au contenu et au délai des réponses fournies par le MROS. Le résultat était positif, tant pour les demandes adressées par le MROS à des CRF étrangères que pour les réponses envoyées par le MROS.

Les réponses des CRF étrangères ont été examinées quant à leur délai et au contenu des informations. Il convient de noter que l'échange d'informations dépend toujours du cadre légal du pays concerné. Il se peut ainsi que certaines informations ne soient disponibles que pour une courte durée (elles ne sont conservées que brièvement) ou que l'échange de certaines informations nécessite une décision de justice. Les échanges bilatéraux et personnels entre le MROS et les autorités partenaires contribuent largement à la qualité des demandes et des réponses des deux côtés. La compréhension mutuelle des possibilités et des obstacles juridiques et matériels s'en trouve encore renforcée.

La durée de traitement des demandes a fait l'objet de nombreuses discussions, car elle peut varier considérablement pour différentes raisons.

³¹ Rapport CDF *Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei*, p. 33 (audit publié le 28 mars 2022, en allemand uniquement)

Les informations – si elles ne figurent pas déjà dans le système d'information en raison d'une communication de soupçons – doivent être obtenues auprès des IF, puis traitées. Il faut en général un certain temps pour que la demande soit abordée. Il n'est pas aisé de la traiter rapidement, d'une part en raison du volume en constante augmentation, d'autre part en raison des nombreuses étapes manuelles nécessaires. Augmenter l'efficacité grâce à une infrastructure informatique moderne revêt également une grande importance pour les échanges internationaux. En comparaison internationale, il apparaît clairement que les CRF ou les pays qui sont avancés techniquement (par ex. en ce qui concerne la consultation de bases de données ou l'accessibilité des registres) répondent plus rapidement. La durée de traitement joue un rôle essentiel dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme et est donc capitale pour que le MROS ne doive pas faire de compromis sur la qualité. L'art. 11a, al. 2^{bis}, LBA, introduit le 1^{er} juillet 2021, a eu pour effet d'augmenter clairement la satisfaction des CRF quant aux réponses du MROS. Ce nouvel article permet au MROS de contacter les IF et de leur demander de lui transmettre les informations requises, même si le système d'information ne contient aucune communication de soupçons à ce sujet.

2.8 Crypto Symposium du MROS

Le MROS reçoit de plus en plus de communications de soupçons liées aux cryptomonnaies. Le nombre d'IF exerçant une activité de PSAV s'est multiplié ces dernières années³². Afin de mettre en évidence les enjeux qui en découlent et d'en débattre, le MROS a organisé pour la première fois une conférence sur la cryptographie le 30 octobre 2023 à Zoug, qui a réuni quelque 160 personnes, représentant principalement des PSAV et des organismes d'autorégulation. Les intervenants, qui se sont exprimés au nom d'autorités nationales et internationales et du secteur privé, ont mis en lumière des thèmes relatifs à la réglementation et à la surveillance ainsi que les

risques liés à l'utilisation des cryptomonnaies. Ils ont abordé les différentes difficultés posées par le suivi des cryptomonnaies incriminées, la lutte contre le blanchiment d'argent et le financement du terrorisme ainsi que la détection des infractions relatives aux cryptomonnaies.

Le SFI a traité des contraintes réglementaires au niveau national et international ainsi que de la classification juridique des cryptomonnaies en Suisse. La FINMA a illustré les obstacles juridiques liés à la surveillance et aux procédures d'application du droit. Le MROS a souligné l'importance de l'identification des risques et donc la nécessité de leur évaluation nationale. La CRF du Luxembourg a relevé la nécessité d'une coopération nationale et internationale dans la lutte contre le blanchiment d'argent, en s'appuyant sur des exemples pratiques de financement du terrorisme. Le Ministère public de Zurich a mis l'accent sur la poursuite pénale de la criminalité organisée liée aux cryptomonnaies. La Guardia di Finanza a complété le tableau en présentant de nouvelles approches et méthodes d'investigation relatives aux cryptomonnaies, y compris le métavers. La conférence s'est conclue par l'exposé d'un cabinet d'avocats d'affaires qui, à l'aide d'exemples tirés de la pratique, a fait le lien entre le secteur privé et les autorités et relevé la complexité du sujet du point de vue des conseillers.



Fig. 1: Invitation au Crypto Symposium du MROS

³² Cf. ch. 2.3.

3. Système d'information goAML

Le système d'information goAML, introduit le 1^{er} janvier 2020, est utilisé pour la réception et le traitement électroniques des communications de soupçons. C'est donc un élément central de la stratégie du MROS en matière de numérisation et d'augmentation de l'efficacité. Quatre ans après son introduction, il est bien établi auprès des IF. Son fonctionnement est stable et sa disponibilité élevée. Plus de 96 % des communications de soupçons et des réponses aux demandes d'informations au sens de l'art. 11a LBA sont transmises au MROS par goAML. Cette évolution est réjouissante, d'autant que presque toute la communication avec les IF passe par ce système. Les données sont à chaque fois

transmises de manière structurée. Actuellement, seules les communications de rupture de la relation d'affaires au sens de l'art. 9b LBA³³ sont transmises en nombre accru de manière non structurée par l'intermédiaire du Message Board de goAML. Il s'agit toutefois d'une solution transitoire, car la version 5.2 empêchera toute transmission non structurée : les IF devront alors effectuer toutes les transmissions par fichier XML ou par l'interface web.

La qualité des données transmises par les IF est encore insuffisante. Si le taux de rejet a baissé à 10 % en 2023³⁴, une transmission sur dix est encore renvoyée aux IF pour non-respect des exigences en la matière.

³³ L'IF peut rompre la relation d'affaires 40 jours ouvrables après avoir envoyé une communication de soupçons pour autant que le MROS ne lui ait pas notifié qu'il transmettait les informations communiquées à une autorité de poursuite pénale. Le cas échéant, il doit informer le MROS de la rupture de la relation d'affaires (cf. art. 9b, al. 3, LBA).

³⁴ Années précédentes : 14 % en 2022, 24 % en 2021, 41 % en 2020

Tabl. 1: Informations reçues par le MROS en 2023

Informations reçues en 2023 (date de référence : 31.12.2023)	Total (nombre)	Non structuré : par courrier postal ou courriel sécurisé ³⁵	Part en % par catégorie	Part en % du total
Tous les rapports nationaux et internationaux *	21 375	5 857		
Ensemble des rapports nationaux	19 944	4 426	–	22,2 %
Expéditeur : IF	16 436	1 502	9,1 %	7,5 %
• Communications de soupçons ³⁶	11 876	158	1,3 %	
• Réponses des IF à une demande au sens de l'art. 11a LBA ³⁷	1 891	70	3,7 %	
• Communications de rupture de la relation d'affaires ³⁸	2 669	1 274	47,7 %	
Expéditeurs : autorités nationales	3 508	2 924	83,4 %	14,7 %
• Autorités de poursuite pénale (dont par courrier)	2 643	2 643 (1 799)	100 % 68 %	
(dont par courriel sécurisé)		(844)	32 %	
• Autres autorités	865	281	32,5 %	

* Les chiffres comprennent également les demandes d'information internationales entrantes ainsi que les informations spontanées des CRF étrangères.

Alors que les IF ne soumettent des données non structurées que dans 9 % des cas, cette part dépasse 80 % pour les autorités nationales. Ces données sont envoyées au MROS soit par courrier postal, soit par le Message Board, la part d'envois postaux étant de 68 % pour les autorités nationales. Le travail de saisie manuelle incombe alors au MROS, ce qui continue de mobiliser des effectifs. Le MROS est en contact avec les autorités de poursuite pénale et continuera à se concerter avec elles en 2024 pour réduire la part de données non structurées à moyen terme. À l'été de 2023, le MROS a introduit la version 5.2 de goAML (censée remplacer la version 4.9), dans un premier temps uniquement en interne à des fins de test en vue de son déploiement ultérieur. Ce changement requerra en 2024 des adaptations de nature informatique pour les IF, qui en ont été informés en décembre 2023. Afin de garantir une transition fluide, le MROS leur a transmis les exigences techniques et a mis en place un environnement de test. D'ici à la fin de

2024, tous les IF devront être passés de l'ancien schéma XSD au nouveau. Pendant cette phase, le MROS continuera d'accepter les anciens fichiers XML. La nouvelle version de goAML renforcera la capacité d'analyse du MROS. Lors de la programmation de la version 5.2, l'ONUUDC³⁹ a tenu compte de nombreuses demandes et exigences du MROS. Cette version simplifiera le traitement des données tant pour les IF que pour les analystes financiers du MROS.

³⁵ Le système goAML dispose d'une fonction de messagerie sécurisée (Message Board) qui assure le chiffrement de bout en bout de la communication entre les parties enregistrées dans goAML et le MROS.

³⁶ Communications de soupçons fondées sur l'obligation de communiquer (art. 9 LBA) et le droit de communiquer (art. 305^{ter}, al. 2, CP).

³⁷ Il s'agit de toutes les demandes au sens de l'art. 11a LBA (al. 1, 2 et 2^{bis}).

³⁸ Communications de rupture de la relation d'affaires au sens de l'art. 9b LBA.

³⁹ Office des Nations Unies contre la drogue et le crime.

4. Statistique annuelle du MROS

Le MROS établit une statistique anonymisée afin d'exploiter les informations concernant le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée et le financement du terrorisme au cours de l'exercice sous revue⁴⁰. Cette statistique comprend notamment les communications de soupçons reçues des IF, les demandes de renseignements d'autorités étrangères analogues ainsi que les procédures faisant suite aux communications (cf. art. 23, al. 1, OBCBA⁴¹).

4.1 Constatations générales 2023

- Le volume des **communications de soupçons** reçues a encore nettement augmenté en 2023 : le MROS en a reçu **11 876**, soit environ 47 par jour ouvrable. Par rapport à 2022 (7639), ce volume représente une augmentation de 55,5%. Depuis que goAML a été introduit en janvier 2020, ce nombre a même plus que doublé (cf. Fig. 2).
- Les communications de soupçons proviennent pour **90,5%** d'IF du **secteur bancaire** (moyenne 2014–2023 : 89,4%).
- En 2023, le MROS a transmis **866 dénonciations aux autorités de poursuite pénale**, soit une baisse de 29,7% (1232) par rapport à l'année précédente ; les dénonciations étaient toutefois plus conséquentes (cf. ch. 4.7). Le nombre moyen de communications

de soupçons transmises aux autorités de poursuite pénale par dénonciation a augmenté (1,8 en 2023, 1,4 en 2022). Le MROS transmet aux autorités de poursuite pénale un rapport d'analyse contenant les informations pertinentes. Celles-ci peuvent être issues de différentes communications de soupçons, qui n'ont pas forcément été transmises au MROS la même année, et provenir de différentes autorités suisses ou étrangères.

- Le nombre de **demandes d'information** au sens de l'**art. 11a LBA** a encore augmenté (+7,1% par rapport à l'année précédente): le MROS entend apporter un soutien optimal aux autorités de poursuite pénale, ce qui suppose une analyse approfondie de certaines communications. L'art. 11a, al. 2^{bis}, LBA, entré en vigueur en 2021⁴², a pour conséquence que le MROS demande davantage d'informations à des IF n'ayant pas contribué directement à la communication (intermédiaires tiers).
- L'**échange d'informations** entre le MROS et les **autorités suisses** est en augmentation constante: le MROS a reçu d'elles 696 demandes d'informations (+4,3%) en 2023. Parallèlement, il leur a transmis spontanément 200 informations, que ce soit à des autorités de surveillance ou à des autorités chargées de lutter contre le blanchiment

⁴⁰ Exercice: du 1^{er} janvier au 31 décembre de l'année concernée.

⁴¹ Ordonnance sur le Bureau de communication en matière de blanchiment d'argent (OBCBA; RS 955.23).

⁴² L'art. 11a, al. 2 et 2^{bis}, LBA forme la base légale habilitant le MROS à demander la remise d'informations à des intermédiaires tiers, qui n'ont pas effectué de communication (cf. ch. 4.12).

d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme (+13,0%).

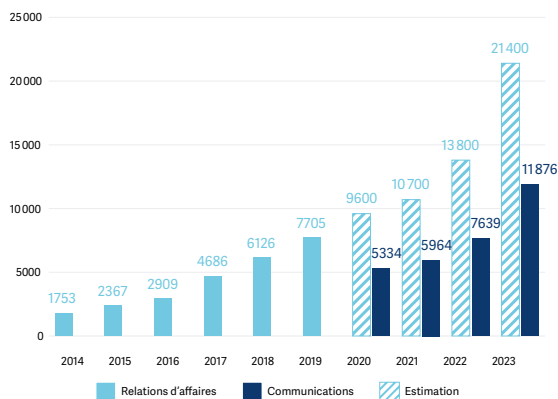
4.2 Communications de soupçons

Le nombre de communications de soupçons augmente d'année en année: le MROS en a reçu 11876 au total en 2023, soit 47 en moyenne par jour ouvrable et une augmentation de 55,5% par rapport à l'année précédente. Ce nombre a même plus que doublé depuis que goAML a été introduit en 2020 (cf. Fig. 2).

L'évolution des relations d'affaires signalées au MROS depuis 2014 est impressionnante: il y en a eu 1753 en 2014, contre environ 21400 en 2023⁴³. Leur nombre annuel a plus que décuplé durant cette période.

Plusieurs raisons expliquent cette augmentation. D'une part, les IF sont de plus en plus sensibles à la problématique du blanchiment d'argent. D'autre part, les adaptations législatives jouent un rôle central, notamment eu égard à la définition du soupçon fondé et aux progrès de la numérisation, comme l'illustre l'amélioration des outils de surveillance des transactions et d'analyse interne (cf. ch. 2.1).

Fig. 2: Nombre de relations d'affaires signalées et de communications de soupçons, 2014–2023

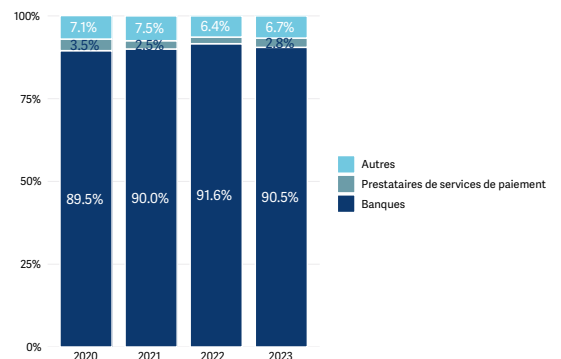


⁴³ La façon de compter les cas suspects a été adaptée avec l'introduction de goAML. Afin de permettre une comparaison avec les années précédentes, la Fig. 2 présente le nombre moyen de relations d'affaires signalées par communication de soupçons transmise en 2019. Ce dernier s'élève à 1,8, ce qui signifie que les 11876 communications de soupçons de 2023 correspondent à environ 21400 relations d'affaires.

4.3 Communications de soupçons par secteur d'activité des IF

La majorité des communications de soupçons adressées au MROS proviennent d'IF du secteur bancaire. Elles représentent 90,5% (-1,1 point de pourcentage par rapport à 2022; cf. Fig. 3). Le comportement de ces IF en la matière influe donc 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.

Fig. 3: Communications de soupçons par secteur, 2020–2023



Le même tableau se dessine pour le nombre de relations d'affaires signalées avant 2020 dans les différents secteurs (cf. Tabl. 2).

Tabl. 2: Communications de soupçons par secteur, 2014–2023⁴⁴

Type d'intermédiaire financier	2014 ¹	2015 ¹	2016 ¹	2017 ¹	2018 ¹	2019 ¹	2020 ²	2021 ²	2022 ²	2023 ²	2023 en chiffres absolus	Moyenne 2014–2023
Banques	85,3%	91,3%	86,0%	91,0%	88,8%	89,9%	89,5%	90,0%	91,6%	90,5%	10744	89,8%
Prestataires de services de paiement	6,1%	2,4%	4,4%	3,1%	4,4%	4,0%	3,5%	2,5%	2,0%	2,8%	328	2,9%
Fiduciaires	2,8%	2,0%	1,5%	1,1%	0,7%	0,8%	0,6%	0,5%	0,1%	0,2%	25	0,8%
Gérants de fortune / Conseillers en placement	2,3%	1,9%	2,2%	1,9%	1,0%	0,9%	0,8%	1,0%	0,6%	0,8%	90	0,8%
Assurances	0,6%	0,5%	3,1%	0,5%	0,6%	0,3%	0,4%	0,3%	0,3%	0,4%	47	0,3%
Autres intermédiaires financiers	0,2%	0,2%	0,7%	0,4%	2,3%	0,6%	2,3%	2,1%	2,1%	2,0%	240	2,1%
Cartes de crédit	0,5%	0,5%	0,7%	0,3%	1,2%	1,3%	1,6%	1,7%	1,6%	1,3%	154	1,5%
Maisons de jeu	0,5%	0,1%	0,5%	0,6%	0,5%	0,7%	0,5%	0,5%	0,7%	0,5%	65	0,6%
Avocats et notaires	0,6%	0,3%	0,2%	0,1%	0,1%	0,1%	0,1%	0,1%	0,0%	0,1%	14	0,1%
Opérations de crédit, de leasing, d'affacturage et de financement à forfait	0,2%	0,3%	0,3%	0,3%	0,3%	0,3%	0,4%	0,3%	0,3%	0,2%	26	0,3%
Maisons de titres	0,6%	0,1%	0,1%	0,3%	0,1%	0,3%	0,0%	0,2%	0,1%	0,2%	22	0,1%
Négociants en matières premières et métaux précieux	0,2%	0,3%	0,1%	0,2%		0,3%	0,2%	0,5%	0,3%	0,3%	38	0,3%
Négoce de devises			0,1%			0,3%	0,0%					0,0%
OAR	0,1%					0,1%	0,0%			0,1%	6	0,0%
Bureaux de change							0,1%	0,1%	0,3%	0,6%	75	0,4%
Autorités (FINMA / CFMJ / GESPA)	0,1%							0,1%		0,0%	2	0,0%
Distributeurs de fonds de placement				0,1%								0,0%
Trustees							0,1%	0,1%				0,0%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	11876	100,0%

¹ D'après l'ancienne manière de compter (par relations d'affaires)

² D'après la nouvelle (ou actuelle) manière de compter (par communications de soupçons)

4.4 Bases légales des communications

La base légale d'une communication de soupçons dépend du degré de suspicion. S'ils ont des soupçons fondés, les IF ont l'obligation de les

communiquer au MROS en vertu de l'art. 9, al. 1, let. a, LBA⁴⁵. 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, CP⁴⁶. Depuis 2018, l'obligation de communiquer gagne en importance par

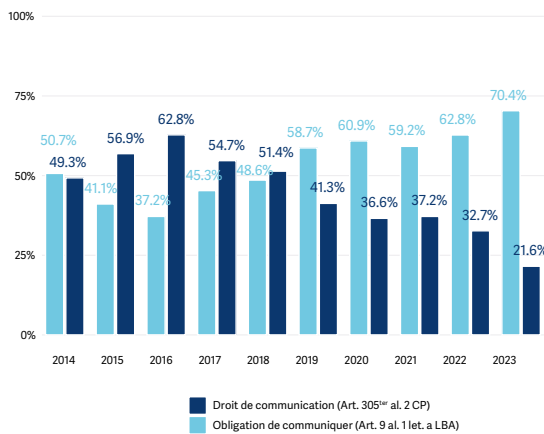
⁴⁴ Les chiffres absolus pour les années 2014 à 2022 sont présentés dans les *rapports annuels du MROS* des années correspondantes.

⁴⁵ L'intermédiaire financier informe immédiatement le Bureau de communication en matière de blanchiment d'argent au sens de l'art. 23 (bureau de communication) s'il sait ou présume, sur la base de soupçons fondés, que les valeurs patrimoniales impliquées dans la relation d'affaires: 1. ont un rapport avec une des infractions mentionnées aux art. 260^{ter} ou 305^{bis} CP, 2. proviennent d'un crime ou d'un délit fiscal qualifié au sens de l'art. 305^{bis}, ch. 1^{bis}, CP, 3. sont soumises au pouvoir de disposition d'une organisation criminelle ou terroriste, 4. servent au financement du terrorisme (art. 260^{quinquies}, al. 1, CP) (art. 9, al. 1, let. a, LBA).

⁴⁶ 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).

rapport au droit de communiquer. Cette évolution s'est encore accentuée en 2023, où les communications transmises relevaient dans 70,4% des cas de l'obligation de communiquer et dans 21,6% du droit de communication. L'utilisation de ce dernier a encore nettement diminué par rapport à l'année précédente (-9,1 points de pourcentage). On peut supposer que l'obligation de communiquer a gagné en importance au cours de 2023 par suite notamment de l'entrée en vigueur de la révision de la LBA au 1^{er} janvier 2023 : l'art. 9, al. 1^{quarter}, LBA définit désormais le soupçon fondé⁴⁷.

Fig. 4: Communications relatives à des relations d'affaires existantes par base légale, 2014–2023



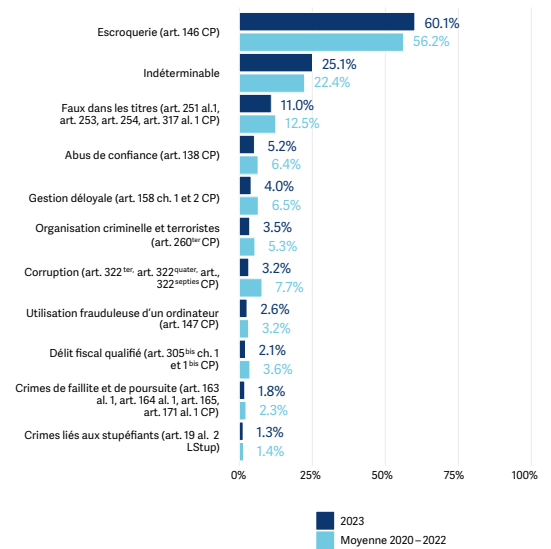
Dans 941 cas (7,9%), les IF ont en outre signalé qu'ils avaient rompu des négociations visant à établir une relation d'affaires en raison d'un soupçon fondé au sens de l'art. 9, al. 1, let. a, LBA⁴⁸.

4.5 Infractions préalables

Lors d'une communication, les IF indiquent à chaque fois les infractions préalables qu'ils présumant. Peu de choses ont changé depuis 2020 dans la fréquence des infractions préalables

présumées (cf. Fig. 5). Ainsi, les dix premières sont les mêmes en 2023 qu'en 2020. L'escroquerie est la plus souvent citée (60,1% en 2023, 56,2% en 2020–2022).

Fig. 5: Fréquence des infractions préalables présumées, 2020–2023, Plusieurs réponses possibles



On constate une légère tendance des IF à citer davantage l'escroquerie, tandis que la corruption ou la gestion déloyale perdent de l'importance. Les chiffres disponibles ne permettent pas de déterminer si cette évolution est due à un changement de comportement des IF en matière de communication ou à une transformation des infractions préalables réelles sous-jacentes. De manière générale, les informations fournies par les IF sur les infractions préalables présumées ne permettent pas de déduire les infractions préalables au blanchiment d'argent effectivement commises. Les présents chiffres indiquent simplement les infractions présumées par les IF au moment où ils ont effectué leurs

⁴⁷ L'art. 9, al. 1^{quarter}, LBA dispose qu'il y a des soupçons fondés au sens de l'art. 9, al. 1, let. a, lorsque l'intermédiaire financier dispose d'un signe concret ou de plusieurs indices laissant supposer que les critères définis à l'al. 1, let. a, pourraient être remplis pour les valeurs patrimoniales impliquées dans la relation d'affaires et que les clarifications supplémentaires effectuées en vertu de l'art. 6 ne permettent pas de dissiper les soupçons.

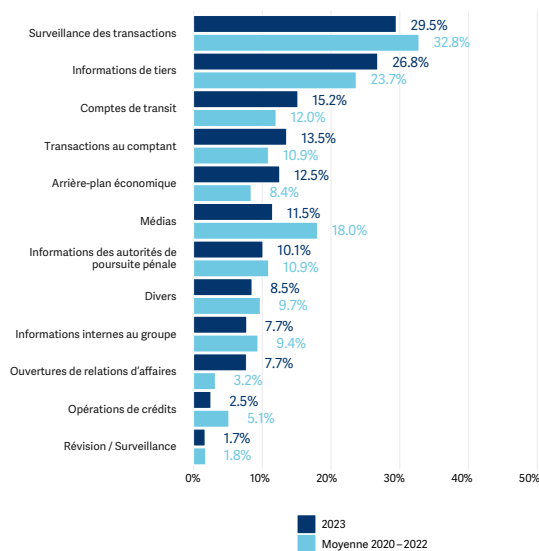
⁴⁸ L'intermédiaire financier informe immédiatement le Bureau de communication en matière de blanchiment d'argent s'il rompt des négociations visant à établir une relation d'affaires en raison de soupçons fondés conformément à la let. a (art. 9 al. 1, let. b, LBA).

communications de soupçons. L'analyse faite par le MROS peut aussi établir des soupçons laissant présumer une autre infraction. Une analyse plus fine des différents types d'infractions préalables a été réalisée sous l'égide du GCBF en 2022⁴⁹.

4.6 Éléments à l'origine des soupçons

Comme les années précédentes, on constate en 2023 que les IF envoient le plus souvent une communication de soupçons au MROS en raison de la surveillance des transactions (29,5% en 2023, 32,8% en 2020–2022; cf. Fig. 6). Dans 15,2% des communications reçues en 2023, des comptes de passage étaient à l'origine d'un soupçon. Toutefois, les sources d'information externes jouent également un rôle essentiel dans l'évaluation des IF: 26,8% des communications de soupçons de 2023 ont été effectuées sur la base d'informations de tiers (23,7% en 2020–2022).

Fig. 6: Principaux éléments à l'origine des soupçons, 2020–2023⁵⁰, Plusieurs réponses possibles



4.7 Dénonciations aux autorités de poursuite pénale

En 2023, le MROS a transmis 866 dénonciations aux autorités de poursuite pénale en vertu de l'art. 23, al. 4, LBA, soit un recul de 29,7% par rapport à l'année précédente (1232 en 2022). Les dénonciations de 2023 sont plus conséquentes que l'année précédente: alors qu'une dénonciation reposait en moyenne sur 1,4 communication des IF en 2022, elle s'appuie en moyenne sur 1,8 communication en 2023.

Les 866 dénonciations transmises contiennent des informations provenant de:

- 1201 communications reçues en 2023;
- 276 communications reçues en 2022;
- 28 communications reçues en 2021;
- 12 communications reçues en 2020;
- 5 relations d'affaires signalées en 2019;
- 3 relations d'affaires signalées en 2018;
- 2 relations d'affaires signalées en 2017.

Cette année encore, il apparaît que la taille du secteur financier d'un canton a une influence significative sur le nombre de dénonciations adressées au ministère public compétent (cf. Tabl. 3). En 2023, le MROS a adressé la plupart des dénonciations aux ministères publics des cantons de Genève (17,6%) et de Zurich (16,3%), comme les années précédentes. Le MPC arrive en troisième position, avec 13,0%, ce qui correspond à une hausse de 6,6 points de pourcentage par rapport à l'année précédente.

⁴⁹ Cf. Groupe de coordination interdépartemental pour la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF): *Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse*, octobre 2021, pp. 17 à 29

⁵⁰ Contrairement à ce qui prévalait avant 2020, le nouveau système d'information goAML permet aux intermédiaires financiers de signaler plusieurs éléments qui les ont portés à concevoir des soupçons. Par contre, il n'est plus possible d'effectuer une comparaison précise de ces chiffres avec ceux des années antérieures à 2020.

Tabl. 3: Dénonciations transmises par autorité de poursuite pénale, 2020–2023

Autorité	2020	2021	2022	2023	2023 en chiffres absolus	Moyenne 2020–2023
Genève	11,5%	11,3%	11,6%	17,6%	152	13,0%
Zurich	18,9%	21,1%	20,4%	16,3%	141	19,2%
MPC	9,0%	9,1%	6,4%	13,0%	113	9,4%
Vaud	11,1%	11,6%	10,6%	8,3%	72	10,4%
Berne	7,5%	6,7%	6,9%	6,5%	56	6,9%
Saint-Gall	3,5%	4,0%	6,3%	5,3%	46	4,8%
Tessin	5,0%	4,8%	3,6%	4,6%	40	4,5%
Argovie	5,3%	5,2%	6,7%	4,2%	36	5,3%
Thurgovie	3,0%	2,1%	2,6%	3,2%	28	2,7%
Lucerne	3,5%	2,9%	2,6%	2,5%	22	2,9%
Valais	2,7%	2,4%	3,0%	2,2%	19	2,6%
Zoug	2,5%	2,6%	2,2%	2,2%	19	2,4%
Schwyz	1,0%	1,1%	1,9%	2,1%	18	1,5%
Bâle-Ville	2,6%	2,3%	2,3%	1,8%	16	2,3%
Bâle-Campagne	2,1%	1,7%	2,3%	1,8%	16	2,0%
Soleure	1,9%	2,0%	2,1%	1,4%	12	1,8%
Fribourg	2,7%	3,1%	2,1%	1,3%	11	2,3%
Neuchâtel	2,3%	1,9%	1,7%	1,3%	11	1,8%
Appenzell Rhodes-Extérieures	0,6%	0,8%	1,3%	0,9%	8	0,9%
Schaffhouse	0,5%	0,5%	0,6%	0,7%	6	0,6%
Jura	0,3%	1,0%	0,2%	0,7%	6	0,6%
Grisons	1,5%	1,0%	1,1%	0,6%	5	1,0%
Nidwald	0,3%	0,4%	0,6%	0,6%	5	0,5%
Glaris	0,2%	0,1%	0,4%	0,6%	5	0,3%
Appenzell Rhodes-Intérieures	0,0%	0,1%	0,2%	0,2%	2	0,1%
Uri	0,3%	0,1%	0,2%	0,1%	1	0,2%
Obwald	0,2%	0,1%	0,2%	0,0%	0	0,1%
Total	100,0%	100,0%	100,0%	100,0%	866	100,0%

Au total, le MROS a transmis 13,0% des dénonciations pénales (113) au MPC et 87,0% (753) aux ministères publics cantonaux.

4.8 Retour des autorités pénales

Conformément à l'art. 29a LBA, les autorités pénales annoncent sans délai au MROS toutes

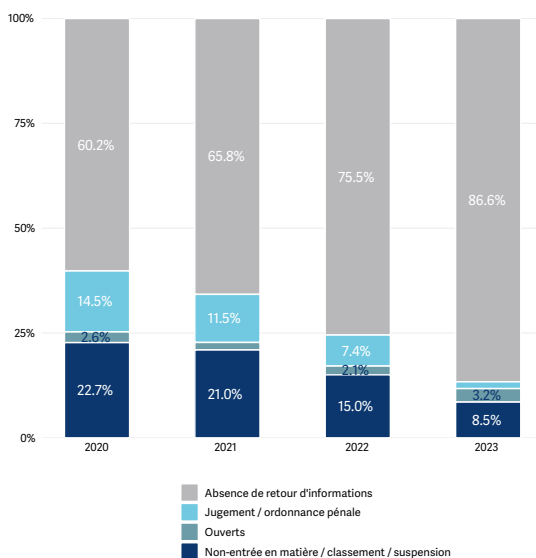
les procédures pendantes en rapport notamment avec le blanchiment d'argent, les organisations criminelles et terroristes et le financement du terrorisme. Elles lui font parvenir sans délai les jugements et les décisions de non-lieu correspondants⁵¹. De plus, elles lui annoncent sans délai les décisions qu'elles ont prises sur les dénonciations qu'il leur a adressées⁵². Ce retour

⁵¹ Les autorités pénales annoncent sans délai au bureau de communication toutes les procédures pendantes en rapport avec les art. 260^{ter}, 260^{quinquies}, al. 1, 305^{bis} et 305^{ter}, al. 1, CP. Elles lui font parvenir sans délai les jugements et les décisions de non-lieu correspondants, y compris leur motivation. (art. 29a, al. 1, LBA).

⁵² Art. 29a, al. 2, LBA.

des autorités pénales est essentiel à la mission du MROS, qui est d'apporter le meilleur soutien possible aux autorités de poursuite pénale. Le retour d'information des autorités pénales est encore attendu pour une majorité de dénonciations (cf. Fig. 7 ainsi que l'explication au ch. 6.2). Il n'est donc pas possible de tirer des enseignements sur le rapport entre les jugements et les décisions de non-lieu à partir des chiffres disponibles actuellement.

Fig. 7: Retour d'information sur les dénonciations transmises au cours de l'année, 2020–2023

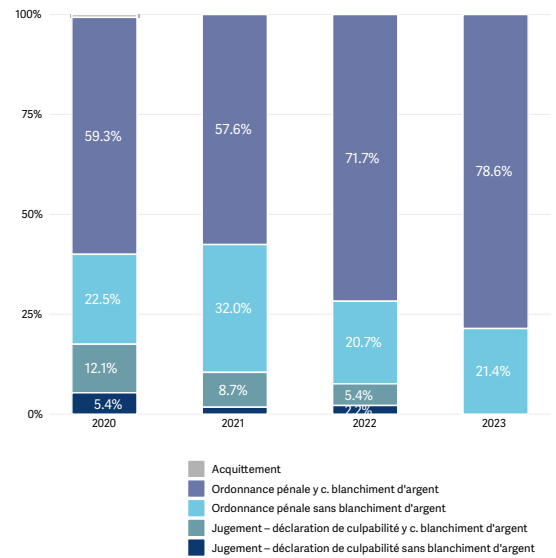


Pour les dénonciations transmises entre 2020 et 2022⁵³, le MROS ne dispose pas, dans deux tiers des cas, d'indication sur l'état d'avancement de la procédure, le taux de retour des autorités pénales variant considérablement d'un canton à l'autre.

Parmi les retours adressés au MROS jusqu'à la fin de 2023 et ayant donné lieu à une ordonnance pénale ou à un jugement, le blanchiment d'argent

était l'infraction principale (78,6%; cf. Fig. 8). En 2022, 77,1% des jugements ou des ordonnances pénales avaient un lien avec le blanchiment d'argent, contre 66,3% en 2021 et 71,4% en 2020.

Fig. 8: Répartition des jugements et des ordonnances pénales communiqués, 2020–2023



4.9 Financement du terrorisme

En 2023, le MROS a reçu 93 communications relatives à des soupçons de financement du terrorisme ou d'infraction à la loi fédérale interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées⁵⁴, ce qui représente 0,8% de toutes les communications reçues. La plupart d'entre elles sont en outre liées à d'autres infractions préalables. Les motifs de suspicion supplémentaires étaient l'appartenance à une organisation criminelle ou terroriste⁵⁵ dans 30 cas, l'escroquerie⁵⁶ dans sept cas, et le délit fiscal

⁵³ Pour tenir compte du fait que le retour d'information des autorités pénales au MROS prend un certain temps, les chiffres de l'année sous revue ne sont pas pris en compte dans la statistique.

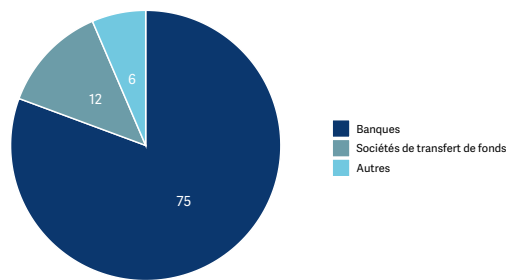
⁵⁴ Loi fédérale du 12 décembre 2014 interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées, RS 122; abrogée le 1^{er} décembre 2022.

⁵⁵ Art. 260^{ter} CP

⁵⁶ Art. 146 CP

qualifié⁵⁷, la corruption⁵⁸, le faux dans les titres⁵⁹ et/ou l'abus de confiance⁶⁰ dans deux cas. La plupart des communications relatives à des soupçons de financement du terrorisme proviennent de banques (75 sur 93; cf. Fig. 9); douze d'entre elles proviennent de prestataires de services de paiement.

Fig. 9: Nombre de communications de soupçons de financement du terrorisme par secteur, 2023



Les éléments à l'origine des soupçons les plus souvent cités par les IF en 2023 étaient les articles de presse (37 cas), la surveillance des transactions (19 cas), ainsi que les informations de tiers (16 cas), de groupes (13 cas) ou d'autorités de poursuite pénale (10 cas), de même que les transactions en espèces (13 cas). Les 93 communications reçues en 2023 ont fait l'objet de cinq dénonciations aux autorités de poursuite pénale compétentes. Trois des communications reçues l'année précédente qui concernaient cette infraction ont également été transmises aux autorités de poursuite pénale compétentes en 2023 pour dénonciation.

4.10 Criminalité organisée

En 2023, le MROS a reçu 421 communications de soupçons concernant des liens avec une organisation criminelle ou terroriste, soit 3,5% de l'ensemble des communications reçues.

⁵⁷ Art. 305^{bis}, ch. 1 et 1^{bis}, CP.

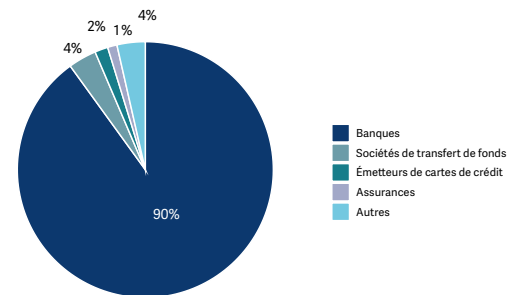
⁵⁸ Art. 322^{ter}, 322^{quater} ou 322^{septies} CP.

⁵⁹ Art. 251, ch. 1, 253, 254 et 317, ch. 1, CP.

⁶⁰ Art. 138 CP.

La grande majorité d'entre elles (90,0%) ont été transmises au MROS par des banques (cf. Fig. 10). Les éléments à l'origine des communications de soupçons étaient des informations provenant des médias (37%) ou une surveillance des transactions (25%; cf. Tabl. 5). Outre le lien présumé avec une organisation criminelle, les IF ont également cité l'escroquerie (44%) et la corruption (8%, cf. Tabl. 4) comme infraction préalable possible. Parmi les 421 communications de l'année sous revue, 33 ont fait l'objet d'une dénonciation aux autorités de poursuite pénale compétentes.

Fig. 10: Communications de soupçons de liens avec une organisation criminelle ou terroriste par secteur, 2023



Tabl. 4: Autres infractions préalables mentionnées dans les communications de soupçons de liens présumés avec une organisation criminelle ou terroriste

Autres infractions préalables (Plusieurs réponses possibles)	Nombre de mentions	En %
Escroquerie (art. 146 CP)	185	44%
Corruption (art. 322 ^{ter} , art. 322 ^{quater} , art. 322 ^{septies} CP)	33	8%
Financement du terrorismes (art. 260 ^{quinquies} CP)	27	6%
Loi sur les stupéfiants (art. 19, al. 2 LStup)	26	6%
Abus de confiance (art. 138 CP)	23	5%
Faux dans les titres (art. 251, ch. 1, art. 253, art. 254, art. 317 al. 1 CP)	18	4%

Autres infractions préalables (Plusieurs réponses possibles)	Nombre de mentions	En %
Délit fiscal qualifié (art. 305 ^{bis} , ch. 1 et 1 ^{bis} , CP)	15	4%
Gestion déloyale (art. 158, ch. 1 et 2, CP)	15	4%
Extorsion (art. 156 CP)	8	2%

Tabl. 5: Fréquence d'autres éléments mentionnés dans les communications de soupçons de liens présumés avec une organisation criminelle ou terroriste

Éléments à l'origine du soupçon (Plusieurs réponses possibles, choix de la fréquence)	Nombre de mentions	En %
Informations des médias	155	37%
Surveillance des transactions	105	25%
Informations de tiers	80	19%
Comptes de transit	49	12%
Divers	46	11%
Transactions au comptant	44	10%
Ouverture de relations d'affaires	43	10%
Informations des autorités de poursuite pénale	38	9%
Arrière-plan économique	31	7%
Informations internes au groupe	25	6%
Opérations de crédits	12	3%

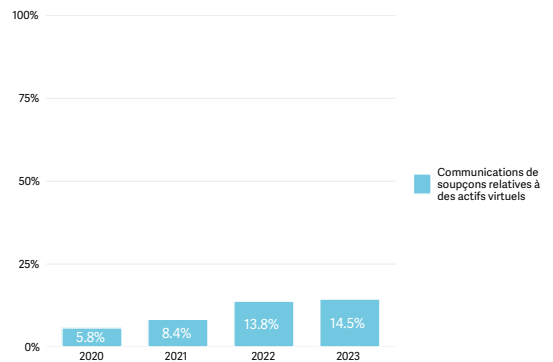
4.11 Communications de soupçons en rapport avec les cryptomonnaies

Les communications de soupçons concernant les cryptomonnaies (ou AV) prennent de plus en plus d'importance⁶¹. En 2023, 14,5% de toutes les communications y étaient liées, soit deux fois et demie plus qu'en 2020 (5,8%; cf. Fig. 11)⁶². Cette évolution pose de plus en plus de difficultés au MROS: les cryptomonnaies compliquent le

suivi des flux financiers et donc l'identification de l'origine des fonds et celle de l'ayant droit économique.

Le MROS a analysé les risques liés aux cryptomonnaies dans le rapport sectoriel relatif au risque de blanchiment d'argent et de financement du terrorisme par les crypto-actifs, qui a été publié au premier trimestre de 2024 (cf. ch. 2.3)⁶³.

Fig. 11: Part des communications relatives aux AV par rapport au total des communications de soupçons, 2020–2023



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

Depuis 2021, le nombre de demandes d'informations adressées aux IF sur la base de l'art. 11a LBA ne cesse d'augmenter. Cette hausse s'est poursuivie en 2023 par rapport à l'année précédente (+7,1%; cf. Fig. 12). Elle est principalement due aux demandes adressées à des intermédiaires tiers qui sont ou ont été concernés par une transaction ou une relation d'affaires en plus de

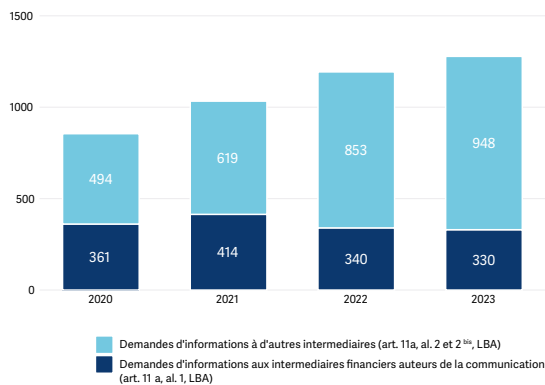
⁶¹ L'art. 4, al. 2, let. a, ajouté le 1^{er} janvier 2016 dans l'ordonnance du 11 novembre 2015 sur le blanchiment d'argent (RS 955.01) a pour la première fois en Suisse inscrit la notion de monnaie virtuelle dans un acte législatif.

⁶² Il n'est pas possible à ce jour de déterminer directement dans quelle mesure les transactions en cryptomonnaies font l'objet d'un soupçon dans une communication, car ces transactions ne sont pas clairement identifiables. Les communications de soupçons présentant un lien pertinent avec les AV ont donc été identifiées, d'une part, au moyen des transactions effectuées entre les comptes affichés dans la communication et les comptes d'IF suisses ou étrangers exerçant une activité de PSAV et, d'autre part, au moyen d'une liste de mots-clés pertinents. On peut donc supposer que l'importance des cryptomonnaies dans les communications de soupçons est plutôt sous-estimée.

⁶³ *National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets* (en allemand uniquement).

l'IF auteur de la communication (+11,1%; art. 11a, al. 2⁶⁴ et 2^{bis} LBA⁶⁵). En revanche, le nombre de demandes adressées aux IF auteurs des communications de soupçons initiales au titre de l'art. 11a, al. 1, LBA⁶⁶ est resté relativement constant (-2,9% par rapport à l'année précédente).

Fig. 12 : Demande de remise d'informations au sens de l'art. 11a LBA, 2020–2023



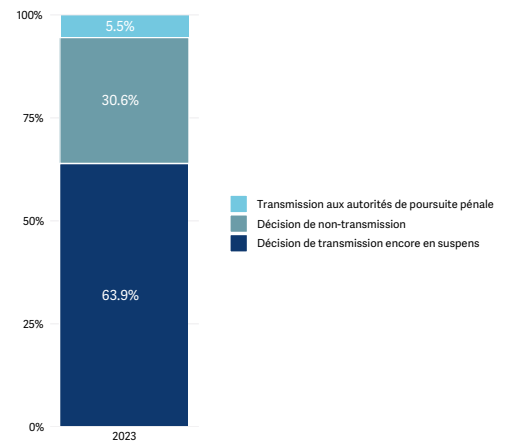
4.13 Communications de rupture de la relation d'affaires au sens de l'art. 9b LBA

Depuis le 1^{er} janvier 2023, les IF peuvent, en vertu de l'art. 9b LBA⁶⁷, 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'IF doit

communiquer sans délai au MROS la rupture de la relation d'affaires⁶⁸.

En 2023, le MROS a reçu 2669 communications de rupture de la relation d'affaires: 5,5% d'entre elles se rapportent à des communications de soupçons qui ont quand même été transmises à une autorité de poursuite pénale après le délai de 40 jours ouvrables, 63,9% à des communications pour lesquelles la décision de transmission est encore en suspens et 30,6% à des communications qui n'ont pas été transmises (cf. Fig. 13).

Fig. 13 : État des communications de soupçons liées à une rupture de la relation d'affaires, 2023



⁶⁴ 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).

⁶⁵ 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).

⁶⁶ Lorsque le bureau de communication a besoin d'informations supplémentaires pour l'analyse d'une communication reçue en vertu de l'art. 9 LBA 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).

⁶⁷ En vertu de l'art. 9b LBA, les IF peuvent rompre une relation d'affaires communiquée en vertu de l'art. 9, al. 1, let. a, LBA ou de l'art. 305^{ter}, al. 2, CP pour autant que le MROS ne leur notifie pas dans un délai de 40 jours ouvrables qu'il transmet les informations communiquées à une autorité de poursuite pénale.

⁶⁸ Art. 9b, al. 3, LBA

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

Dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, le financement du terrorisme et la criminalité organisée, l'échange d'informations entre le MROS et ses homologues étrangers (les CRF) fonctionne au moyen de l'entraide administrative. Lorsque le MROS reçoit des communications de soupçons impliquant des personnes physiques ou morales étrangères, il peut demander des informations à leur sujet aux CRF des pays concernés. Ces informations sont capitales pour ses analyses, car un grand nombre de communications de soupçons ont un lien avec l'étranger⁶⁹. Le nombre de demandes adressées à des CRF étrangères n'a cessé de croître ces dernières années. En 2023, le MROS en a adressé 280 à 67 CRF différentes, soit une augmentation de 6,9% par rapport à l'année précédente.

En juillet 2021, le MROS s'est vu octroyer davantage de compétences en matière d'échange d'informations avec ses homologues étrangers (art. 11a, al. 2^{bis}, LBA). Il a donc reçu beaucoup plus de demandes de bureaux de communication étrangers en 2022 (851 demandes provenant de 89 pays). Le MROS peut depuis lors enrichir ses réponses des informations financières pertinentes. Les demandes et leur traitement en deviennent parfois plus complexes qu'avant 2021. En 2023, le nombre de demandes provenant de 92 pays a de nouveau baissé (705; -17,2%). Le MROS en a traité 350 d'entre elles et 306 de l'année précédente.

Les CRF étrangères et le MROS peuvent également échanger spontanément des informations. Il s'agit là d'un échange sans demande préalable. Durant l'année sous revue, le MROS a reçu 726 informations spontanées de 53 pays (709 de 50 pays en 2022). Le MROS a envoyé 160 informations spontanées à 47 CRF étrangères (178 à 56 CRF étrangères en 2022).

4.15 Échange d'informations avec les autorités suisses

Le MROS échange également, sur demande ou spontanément, des informations pertinentes avec les autorités suisses en vertu de l'art. 29 LBA. Il s'agit d'autorités de surveillance ou d'autres autorités engagées dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme. Les statistiques des années précédentes montrent que les échanges avec ces autorités gagnent en importance depuis 2020⁷⁰. Au cours de 2023, le MROS a reçu 696 demandes d'informations de 29 autorités suisses concernant des comptes bancaires, des personnes ou des entreprises spécifiques, ce qui représente une augmentation de 4,3% par rapport à 2022. Comme les années précédentes, la majorité de ces demandes, soit 82,0%, émanent des autorités policières (polices cantonales et Police judiciaire fédérale).

En outre, le MROS a reçu 119 informations spontanées de la part des autorités suisses en 2023 (109 en 2022). De son côté, il a transmis des informations spontanées aux autorités de surveillance et autres autorités suisses dans 200 cas (+13,0%; 177 en 2022). Il peut également demander auprès d'autres autorités de la Confédération, des cantons et des communes les informations dont il a besoin pour ses analyses; ces demandes ne figurent pas dans les chiffres précités.

⁶⁹ Cf. GCBF: *Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse*, octobre 2021.

⁷⁰ Cf. Office fédéral de la police (fedpol), Publications du Bureau de communication en matière de blanchiment d'argent (MROS), *Rapports annuels du MROS*

5. Typologies⁷¹

Le dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme est complexe. De par sa fonction de plaque tournante, le MROS peut contribuer de manière substantielle à dresser un tableau complet des situations où les informations existantes sont fragmentées. L'utilisation efficace des instruments mis à sa disposition par la législation et la mise en relation des informations dont il dispose lui permettent d'obtenir une vue d'ensemble et créent une réelle valeur ajoutée pour les autorités de poursuite pénale et les autres autorités. Le MROS conçoit ces tâches comme une création de renseignement, qui est également sa fonction principale. Le présent chapitre vise à illustrer, à l'aide d'exemples concrets, ce que le MROS entend par renseignement.

5.1 Typologie 1 – coopération nationale et internationale

Le cas ci-après illustre l'importance de la coopération nationale et internationale dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée et le financement du terrorisme. Ce n'est que par l'échange national et international que les différentes informations contenues dans les systèmes peuvent être rassemblées en une image globale pour aboutir à des conclusions pertinentes.

Étude de cas : soupçon de coup d'État

Au début de 2022, des enquêtes ont été ouvertes en Suisse et à l'étranger sur différentes personnes

soupçonnées de planifier un coup d'État. Au milieu de la même année, le MROS a reçu pour la première fois une demande d'entraide administrative dans le cadre d'une enquête menée à l'étranger. Plus précisément, il s'agissait d'une personne domiciliée en Suisse (A), qui aurait effectué des versements de soutien à la personne visée étrangère (C) par le biais d'un intermédiaire (B). C serait un membre haut placé d'une organisation censée planifier un coup d'État. Peu après, le MROS a reçu une autre demande d'une CRF étrangère dans le même contexte, cette fois-ci à propos de C, qui se trouvait à l'étranger, et de ses relations avec une autre personne résidant en Suisse. Les informations transmises par la CRF indiquaient l'existence d'une relation d'affaires auprès d'un IF suisse. Le MROS a requis et obtenu des informations sur la relation d'affaires en question auprès de l'IF concerné. Il a entamé sa propre analyse et demandé en même temps des informations à la CRF étrangère. Il était important à cet effet qu'il sache s'il existait, concernant l'expéditeur et le bénéficiaire étrangers des fonds, des informations qui relèvent du blanchiment d'argent et des infractions préalables au blanchiment d'argent ou si une procédure pénale était en cours.

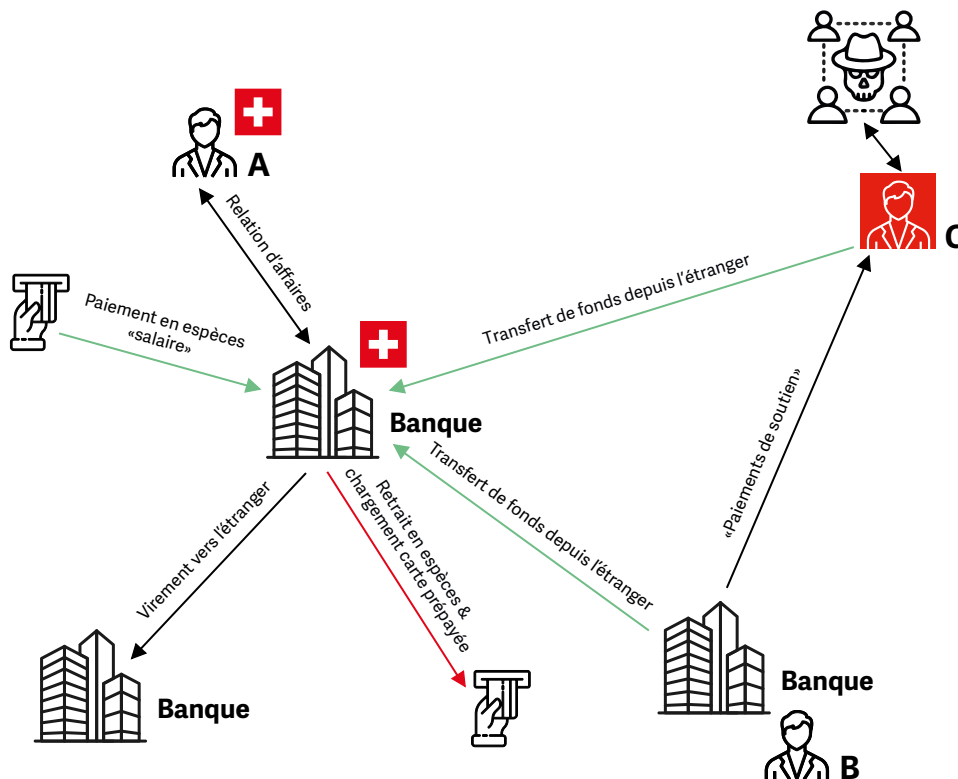
Pour son analyse globale, le MROS a rassemblé les informations nationales et internationales ainsi que les communications de soupçons et dressé le tableau général suivant : A a effectué des versements en espèces inhabituellement nombreux et importants au cours des deux ans et demi précédant la réception de la première communication de soupçons. Il a expliqué ces transactions

⁷¹ La présomption d'innocence s'applique à toutes les personnes concernées.

par le fait qu'il recevait toujours son salaire en espèces. À chaque fois, ces montants étaient soit retirés en espèces peu après leur versement, soit transférés directement à l'étranger. Le MROS a considéré ces comportements comme des transactions de passage. A ne pouvait pas expliquer de manière probante pourquoi une personne étrangère avait accès à son compte personnel et chargeait régulièrement des cartes Travel Cash prépayées avec un montant élevé. En outre, A acceptait des fonds de personnes étrangères qui, grâce aux informations obtenues dans le cadre de la coopération internationale, ont été identifiées comme étant à l'origine du projet de coup d'État. Par ailleurs, le MROS a découvert des liens avec les milieux d'extrême droite en Suisse et à l'étranger. En janvier 2023, le MROS a envoyé une information spontanée à une CRF étrangère, qui a traité les informations de manière consolidée. Le MROS a en outre transmis le rapport d'analyse à l'autorité de poursuite pénale suisse compétente (art. 23, al. 4, LBA), qui a ouvert en mars 2023 une

procédure pénale contre les prévenus domiciliés en Suisse pour participation à une organisation criminelle et terroriste (art. 260^{ter} CP). L'exemple précité illustre qu'une communication de soupçons en soi ou une demande de l'étranger ne sont souvent pas assez substantielles pour identifier une infraction éventuelle. Dans le cas présent, ce n'est en outre pas un IF, mais une CRF étrangère qui porte les faits à la connaissance du MROS. La coopération entre le MROS et les autorités partenaires nationales et internationales et la création de renseignement qui en résulte ont été déterminantes pour la transmission d'informations à l'autorité de poursuite pénale suisse compétente. Ce cas démontre aussi particulièrement bien que les informations transmises au MROS ne sont pas toujours immédiatement révélatrices, mais qu'elles peuvent être pertinentes du point de vue pénal à un stade ultérieur et considérées dans leur ensemble en combinaison avec d'autres informations.

Fig. 14: Typologie 1 – soupçon de coup d'État



5.2 Typologie 2 – utilisation des instruments légaux

L'étude de cas ci-après illustre que le MROS met l'accent sur la lutte contre la grande criminalité lors de l'analyse des communications de soupçons. Ce dernier décide avec quel niveau de détail procéder à l'aide de la matrice de tri. Il met ensuite en œuvre tous les instruments nécessaires prévus par la loi afin de dresser un tableau aussi complet que possible des faits pour l'autorité de poursuite pénale.

Étude de cas : traite d'êtres humains et prostitution forcée

Le MROS a reçu en 2022 une demande d'une CRF étrangère concernant une société X sise en Suisse et l'activité transactionnelle sur ses comptes suisses. On soupçonnait que les fonds issus de différents crimes (notamment la traite d'êtres humains et la prostitution forcée) avaient transité par ses comptes. La CRF étrangère a reçu plusieurs communications de soupçons décrivant le même mode opératoire : un réseau de personnes physiques et morales, domicilié dans une région frontalière de la Suisse, se voyait verser des fonds provenant principalement de personnes physiques du pays Z. Ces valeurs patrimoniales étaient ensuite transférées sur les comptes suisses de la société X. Selon les informations de la CRF étrangère, des contreparties étaient notamment impliquées dans des cas de traite d'êtres humains et de prostitution forcée, ces crimes ayant à chaque fois été commis à l'étranger.

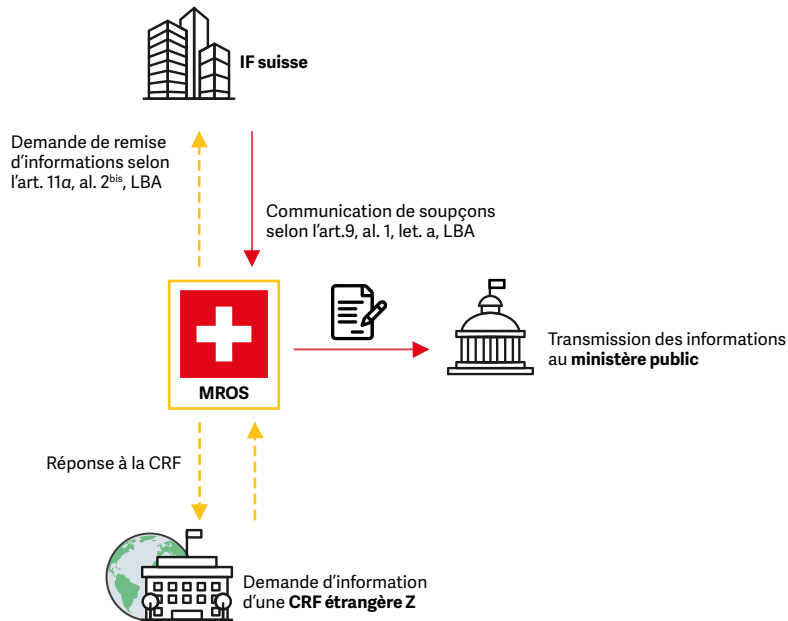
À partir des demandes d'informations des CRF étrangères, le MROS a demandé aux IF suisses concernés, en vertu de l'art. 11a, al. 2^{bis}, LBA, les informations relatives aux comptes suisses en question.

La traite d'êtres humains et la prostitution forcée sont souvent difficiles à détecter sans indices supplémentaires et sur la seule base du comportement transactionnel sous-jacent, car les flux de trésorerie et les virements portent généralement sur de faibles montants. Grâce aux informations fournies par les IF suisses, le MROS a pu établir une analyse détaillée des transactions. Cette dernière a révélé qu'un même groupe

de personnes physiques transférait plusieurs fois par jour la même somme sur les comptes suisses en question. Par la suite, des versements supplémentaires de personnes morales, prenant le relais des personnes physiques, portant sur des montants plus élevés et plus espacés dans le temps étaient effectués. Lors du transfert ultérieur des valeurs patrimoniales, on a constaté notamment que des paiements étaient faits en faveur d'autorités migratoires et d'une agence de voyage domiciliée dans une juridiction sensible eu égard à la traite d'êtres humains et la prostitution forcée. Ces informations ont été communiquées à la CRF étrangère.

À la suite de la demande faite par le MROS en vertu de l'art. 11a, al. 2^{bis}, LBA et sur la base de ses propres clarifications, l'IF lui a adressé une communication de soupçons au sens de l'art. 9, al. 1, let. a, LBA. Toutes les informations ont ensuite été transmises au ministère public cantonal compétent en raison de soupçon de traite d'êtres humains.

Fig. 15: Typologie 2 – traite d’êtres humains et prostitution forcée

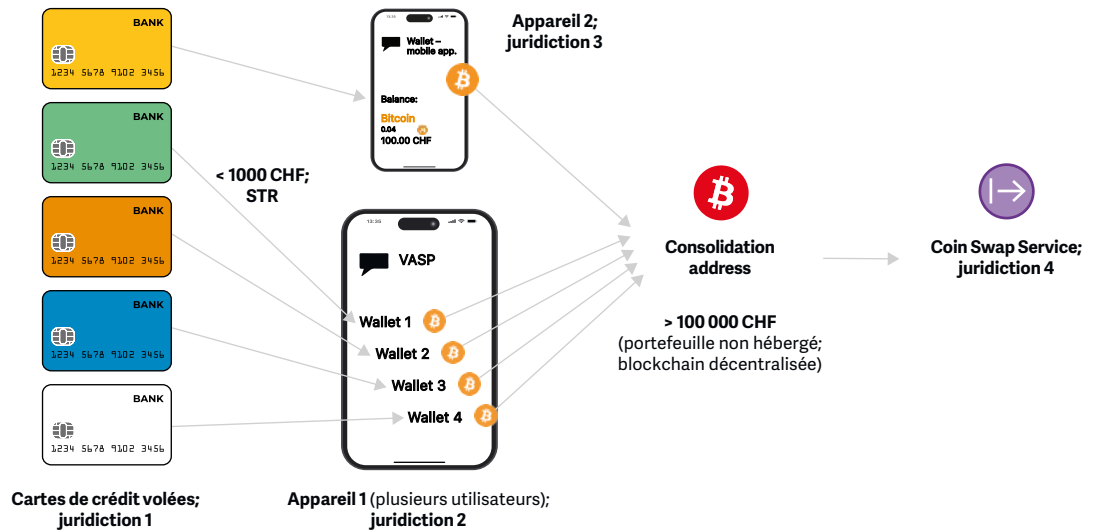


5.3 Typologie 3 – procédure d’analyse globale

Les communications concernant les valeurs patrimoniales virtuelles et les cryptomonnaies ne peuvent souvent être analysées avec succès que si plusieurs cas sont examinés de manière consolidée, en raison de la complexité et du caractère décentralisé et transfrontalier des faits relevant du blanchiment d’argent. L’ensemble de la structure ne peut être identifié que grâce à une procédure d’analyse globale (*cluster*; cf. ch. 2.2). Le cas présent montre une constellation dans laquelle des cas individuels analysés ont été traités comme un cas global de grande envergure. Le MROS a détecté un cas lors d’une analyse, appuyée par des techniques de *blockchain intelligence*, dont le but était l’identification de criminalité sérieuse. Les cas analysés (de manière consolidée) étaient principalement des informations communiquées qui n’avaient jusqu’alors pas fait l’objet d’une transmission d’informations à une autorité de poursuite pénale.

Après analyse, plusieurs communications de soupçons de blanchiment d’argent (*suspicious transaction reports*, STR) ont été identifiées comme impliquant un même groupe d’auteurs présumés (*cluster*). Il s’agissait de STR émises par des IF suisses du type PSAV spécialisés dans l’achat-vente d’actifs virtuels, mais qui ne s’occupaient pas de la gestion des avoirs de leurs clients (*non-custodial*). Les annonces concernaient des soupçons de vols de cartes de crédits émises dans un pays d’Europe de l’Ouest, qui ont été rapportées au MROS après que l’IF a reçu des informations de tiers. Les lésés auraient tous déposé plainte auprès d’une police locale de leur pays après avoir constaté que des achats de bitcoins avaient été effectués indûment au moyen de leur carte de crédit. Les STR concernaient toutes des enquêtes policières étrangères différentes. Le total consolidé de toutes les transactions suspectes communiquées au MROS était inférieur à CHF 1000 (pour ce *cluster*).

Fig. 16: Typologie 3 – procédure d'analyse globale (cluster)



Pour chaque carte de crédit volée, un nouveau compte d'utilisateur avait été créé auprès de l'IF. Pour ces transactions, qui étaient toutes en dessous d'un seuil donné, aucune identification par formulaire Know Your Customer (KYC) n'était requise. Toutefois, d'autres traces informatiques (*logs*) étaient collectées par l'IF (art. 51a OBA-FINMA⁷²).

Lors de l'achat de bitcoins par carte de crédit, l'IF échange par exemple des euros (fiat) contre les bitcoins. Il transfère ensuite la propriété des bitcoins à une adresse que contrôle son client sur la blockchain (technologie de registre distribué), par exemple à un *wallet* se trouvant dans une application installée sur le *smartphone* du client. Ce dernier est le seul à détenir le code secret qui lui permet de disposer de ces fonds. L'IF n'a aucun pouvoir de bloquer les avoirs, par exemple. Ainsi, chaque STR concernait globalement une carte de crédit volée pour une relation d'affaires. Le MROS a connaissance d'une carte de crédit et d'une adresse bitcoin contrôlée par le cocontractant pour chaque transaction. Nous avons pu observer in fine qu'une demi-douzaine au moins de relations d'affaires semblaient avoir été ouvertes

depuis ce qui pourrait être le même *smartphone* (même modèle de téléphone portable, adresse IP géolocalisée dans la même ville d'Europe de l'Est). Une autre relation d'affaires associée au *cluster cible* présentait des caractéristiques différentes. Toutefois, pour toutes ces annonces, l'intégralité des fonds liés aux adresses bitcoin renseignées dans les STR étaient ensuite immédiatement et systématiquement transférés en faveur d'une même contrepartie directe ou adresse bitcoin (1 hop).

Lors de l'analyse menée entre autres à l'aide de différents outils d'analyse de la blockchain, il est rapidement apparu que l'adresse bénéficiaire en question semblait être un *unhosted wallet* utilisé afin de consolider des fonds d'origine criminelle. Cette déduction s'appuie sur le fait que les fonds provenaient de plusieurs centaines de sources différentes et qu'après un certain temps, ils étaient systématiquement transférés par paquets en faveur de ce qui semblait être un PSAV enregistré auprès d'une juridiction offshore. Ce dernier ne semblait pas requérir d'identification KYC de ses utilisateurs. Le MROS a ensuite pu constater, au moment de la recherche, que

⁷² Ordonnance de la FINMA du 3 juin 2015 sur le blanchiment d'argent (RS 955.033.0)

l'adresse avait servi à consolider au total plus d'une centaine de milliers de francs suisses. À ce moment-là, les outils d'analyse de la *blockchain* utilisés ne référençaient pas d'adresses cryptographiques (cluster) associées à l'IF suisse auteur des STR dans les bases de données du MROS. Il n'était donc pas possible de déterminer ainsi si d'autres transactions suspectes provenaient de la même source. Seule une analyse de la *blockchain* plus approfondie⁷³ appuyée par une demande de renseignements (art. 11a LBA) adressée à l'IF a permis d'identifier d'autres utilisateurs potentiels qui auraient transféré des fonds à l'adresse dite de consolidation (en rouge). Il semblait ainsi plausible que d'autres clients de l'IF puissent encore être associés à ce schéma criminel présumé ou qu'un ou plusieurs auteurs présumés aient créé d'autres comptes, sans s'identifier auprès de l'IF. Sur la base de l'échantillon requis, il a également été constaté que les lésés semblaient être localisés dans différents pays du monde.

En l'occurrence, dans cette configuration assez typique, le MROS constate que des lésés sont domiciliés à l'étranger et que les auteurs semblent agir en groupe depuis d'autres juridictions également situées à l'étranger, selon des modèles rendant possibles ou facilitant des escroqueries à plus grande échelle grâce à Internet (*cyber-enabled fraud*). Les fonds dérobés sont ensuite directement convertis en cryptomonnaies auprès d'IF suisses, dans le cas d'espèce en passant au-dessous des seuils d'identification KYC. Les cryptomonnaies d'origine criminelle sont ensuite directement mises à la disposition des auteurs sur des *non-custodial wallets*. Les auteurs présumés ou des blanchisseurs professionnels peuvent ainsi transférer directement les bitcoins à des services à risque relevant d'autres juridictions, afin de convertir le profit de leur crime. Dans ce cas, le MROS a partagé les informations à sa disposition via le canal FIU.

⁷³ Identification de modèles transactionnels.

6. Pratique du MROS

6.1 Interprétation de l'art. 11a LBA – remise d'informations par les IF

L'art. 11a LBA habilite le MROS à demander des informations aux IF lorsque l'analyse des communications effectuées en vertu de l'art. 9 LBA (obligation de communiquer) ou de l'art. 305^{ter}, al. 2, CP (droit de communication) ou sur la base d'informations fournies par des CRF étrangères permet d'établir que les IF concernés ont participé aux faits par le biais de transactions ou de relations d'affaires.

La possibilité de recueillir des informations auprès d'IF en vertu de l'art. 11a LBA est un instrument important pour lutter efficacement contre le blanchiment d'argent, qui est régulièrement pratiqué au moyen de schémas complexes et au-delà des juridictions nationales. Cet instrument permet en effet, d'une part, de replacer les communications de soupçons des IF dans un contexte plus large et, d'autre part, de fournir aux CRF étrangères les informations nécessaires à la lutte contre le blanchiment d'argent.

Lorsque le MROS reçoit des demandes de renseignements de CRF étrangères concernant des relations d'affaires en Suisse, il vérifie au préalable, conformément à l'art. 31 LBA, s'il existe un lien avec la Suisse et s'assure ainsi que les partenaires étrangers ne s'adonnent pas une fishing expedition. Si le client ainsi que l'IF suisse qui gère son compte sont nommément cités par la CRF étrangère, le MROS considère, conformément à sa pratique, que le lien avec la Suisse est suffisant, même en l'absence d'informations

plus précises sur la relation d'affaires, comme des numéros de compte. En revanche, si la CRF étrangère ne fait que supposer l'existence d'une relation d'affaires en Suisse, sans indiquer d'IF précis, le MROS n'entre pas en matière sur sa demande.

S'il obtient des informations sur certains comptes, le MROS se renseigne régulièrement sur l'existence d'autres comptes éventuels au sein de la même relation d'affaires : les co-contractants, les ayants droit économiques ou les personnes ou sociétés liées peuvent en effet jouer un rôle clé. Dans certains cas, il sait seulement qu'il existe une relation d'affaires entre une personne ou une société et une banque, mais ne dispose pas d'informations, ni sur le numéro de la relation d'affaires, ni sur les numéros de compte, ni sur les transactions. Il demande alors aux IF de lui fournir des informations sur la relation d'affaires en question, en indiquant uniquement la personne ou la société titulaire. Une remise d'informations rapide et complète de la part des IF est indispensable pour lutter efficacement contre le blanchiment d'argent aux niveaux national et international.

Les IF sont tenus de mettre à la disposition du MROS toutes les informations pertinentes en leur possession. La loi ne leur accorde pas de marge d'appréciation concernant la proportionnalité de la demande, ni la possibilité d'une contestation ou d'une mise sous scellés. Ils doivent donc fournir les informations demandées dans le délai fixé par le MROS⁷⁴.

⁷⁴ Art. 11a, al. 3, LBA.

Si un IF n'accède pas à la demande du MROS, ce refus peut constituer une violation du droit de la surveillance. En vertu de l'art. 10, al. 2, OBCBA, le MROS peut informer l'autorité de surveillance, l'organisme de surveillance ou l'organisme d'autorégulation compétent au sens de l'art. 29, al. 1, ou 29b LBA des infractions éventuelles au droit de la surveillance commises par les IF, ce qu'il fait régulièrement. Il incombe alors à ces derniers d'enquêter sur de telles violations potentielles du droit de la surveillance et, le cas échéant, de prendre les mesures qui s'imposent.

6.2 Interprétation de l'article 29a LBA – annonce des jugements et des décisions par les autorités pénales

L'art. 29a, al. 1, LBA oblige toutes les autorités pénales⁷⁵ à annoncer au MROS les jugements et les ordonnances de non-lieu, y compris leur motivation, concernant des procédures en rapport avec les art. 260^{ter}, 260^{quinquies}, al. 1, 305^{bis} et 305^{ter}, al. 1, CP. Les jugements et les ordonnances de non-lieu donnent au MROS une vue d'ensemble des développements en matière de blanchiment d'argent, d'infractions préalables au blanchiment d'argent, de criminalité organisée et de financement du terrorisme et l'aident à sensibiliser les IF à cette problématique. En outre, les autorités pénales doivent, conformément à l'art. 29a, al. 2, LBA, lui notifier toutes les décisions qu'elles ont rendues sur la base d'une dénonciation de sa part. La liste des jugements et des décisions à lui annoncer comprend notamment :

- l'ouverture d'une instruction (art. 309, al. 3, CPP);
- les ordonnances de non-entrée en matière (art. 310, al. 1, CPP);
- les décisions concernant l'extension de l'instruction (art. 311, al. 2, CPP);
- les suspensions (art. 314 CPP);
- la reprise de l'instruction (art. 315 CPP);

- les ordonnances pénales (art. 353 CPP);
- les ordonnances de classement (art. 320 CPP);
- la reprise de la procédure préliminaire (art. 323 CPP);
- les jugements (par ex. au sens des art. 351 ou 408 CPP).

Le MROS est ainsi informé de l'avancement des procédures, mais il peut aussi transmettre rapidement à l'autorité compétente les informations issues d'autres communications éventuelles concernant les mêmes faits et tenir les statistiques pertinentes. Il peut en outre tirer des enseignements de son travail, eu égard notamment à sa pratique en matière de transmission aux autorités de poursuite pénale.

L'obligation prévue à l'art. 29a LBA comprend également la transmission spontanée d'informations au sens de l'art. 67a de la loi sur l'entraide pénale internationale⁷⁶, ces informations ayant pour but de permettre de présenter une demande d'entraide pénale spécifique à la Suisse. Dans son audit du 20 décembre 2021 sur la réalisation des tâches du MROS⁷⁷, le CDF regrette, eu égard à l'art. 29a, al. 1 et 2, LBA, que le MROS dispose de données incomplètes sur les décisions rendues par les autorités pénales en matière de blanchiment d'argent, particulièrement lorsque ces décisions sont liées à une communication de soupçons. Le CDF relève que le retour d'information des autorités de poursuite pénale cantonales est lacunaire, voire insatisfaisant : *« Le MROS n'a pas de vue d'ensemble de la chaîne de processus et du cycle de vie de ses communications de soupçons, ce qui serait pourtant déterminant pour évaluer l'efficacité et l'amélioration de son propre travail. Il déplore depuis 20 ans que le MPC, les ministères publics cantonaux et les instances des tribunaux appelés à juger ne respectent pas l'obligation légale prévue par l'art. 29a LBA. À l'image de la comparaison systéma-*

⁷⁵ Le terme d'autorités pénales englobe aussi bien les autorités de poursuite pénale cantonales que le MPC ainsi que toutes les instances des tribunaux appelés à juger (Message sur la mise en œuvre des recommandations révisées du Groupe d'action financière [GAFI], FF 2007 5919, 5953).

⁷⁶ Loi du 20 mars 1981 sur l'entraide pénale internationale (RS 351.1).

⁷⁷ Rapport CDF *Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei*, p. 33 (audit publié le 28 mars 2022, en allemand uniquement)

tique pratiquée depuis 2020 avec le MPC, lesdits ministères et instances devraient également se conformer à cette prescription légale.»

À la faveur de la critique formulée par le CDF, le MROS a rappelé aux autorités pénales leur obligation en la matière durant l'année sous revue. Les statistiques présentées au ch. 4.8 montrent qu'il subsiste un potentiel d'amélioration. Le MROS a besoin du retour d'information le plus complet possible pour évaluer efficacement les informations visées à l'art. 29a LBA et apporter la valeur ajoutée qu'on attend de lui en matière de lutte contre la criminalité et de prévention.

7. Coopération internationale en matière de lutte contre le blanchiment d'argent

7.1 Groupe Egmont

Le MROS est membre du Groupe Egmont depuis 1998. Ce dernier est un réseau international qui regroupe 173 CRF opérationnellement indépendantes et spécialisées dans la détection du blanchiment d'argent, des infractions préalables au blanchiment d'argent et du financement du terrorisme, ainsi que dans la lutte contre ces phénomènes. Il applique les normes fixées par le GAFI, principal organe international de lutte contre le blanchiment d'argent et le financement du terrorisme (cf. ch. 7.2). Il permet, au niveau opérationnel, l'échange d'informations conçu selon les principes du GAFI entre les CRF des différents pays membres. Depuis que les recommandations du GAFI ont été révisées en 2012, l'adhésion au Groupe Egmont est la condition indispensable d'un système efficace de lutte contre le blanchiment d'argent et le financement du terrorisme.

Les objectifs du Groupe Egmont sont notamment les suivants :

- créer les conditions nécessaires à un échange d'informations international systématique ;
- aider les CRF à accroître leur efficacité en développant des stratégies de formation et en encourageant les programmes d'échange destinés aux collaborateurs ;
- permettre l'échange d'informations international entre les CRF en toute sécurité ;
- assurer l'indépendance opérationnelle des CRF ;
- contribuer à la mise en place de bureaux de communication centralisés.

Les responsables des CRF (Heads of FIU) constituent l'organe de direction du Groupe Egmont. Une réunion plénière (Plenary) où les décisions importantes sont discutées et prises en commun a lieu une fois par an dans des lieux différents. Les responsables de CRF sont épaulés par le Comité Egmont, organe consultatif de coordination, et par le Secrétariat du Groupe Egmont, dont le siège est situé au Canada.

Le Groupe Egmont comprend quatre groupes de travail :

- « **Information Exchange Working Group** » (**IEWG**) : ce groupe de travail a pour mission d'identifier les synergies opérationnelles et stratégiques entre les différentes CRF et de veiller à ce qu'elles soient exploitées en conséquence. Il veille également à améliorer en permanence la coopération et l'échange d'informations.
- « **Membership, Support and Compliance Working Group** » (**MSCWG**) : ce groupe de travail veille à ce que les principes du Groupe Egmont soient respectés par les CRF, qu'il s'agisse de nouveaux membres ou de membres existants.
- « **Policy and Procedures Working Group** » (**PPWG**) : ce groupe s'occupe des questions stratégiques, y compris l'échange d'informations efficace entre les CRF et le respect des normes internationales (GAFI).
- « **Technical Assistance and Training Working Group** » (**TATWG**) : ce groupe de travail est chargé d'identifier, de mettre au point et de fournir une assistance technique et des possibilités de formation à toutes les

CRF – membres existants et CRF en cours d'adhésion – ainsi qu'à toutes les organisations observatrices et autres partenaires internationaux du Groupe Egmont.

Ces quatre groupes de travail sont chacun dirigés par un président et un ou plusieurs présidents suppléants issus de différentes CRF. Des réunions auxquelles le MROS participe sont organisées régulièrement (réunions plénières, groupes de travail et réunions régionales). Lors des réunions régionales, les CRF sont affectées à un groupe en fonction de critères géographiques. Les CRF européennes sont réparties en deux groupes : le groupe Europe I comprend les CRF des pays membres de l'UE, tandis que toutes les autres CRF, y compris le MROS, sont affectées au groupe régional Europe II⁷⁸. Ces groupes régionaux permettent d'appréhender les défis et les problématiques spécifiques à une région.

Rencontre avec les membres du Groupe Egmont

Une réunion de travail et de groupe régional, qui s'est tenue à Dakar, au Sénégal, du 30 janvier au 3 février 2023, a regroupé 287 délégués et douze observateurs et partenaires internationaux. Quinze réunions au total ont été organisées afin de renforcer les capacités des membres du Groupe Egmont, d'améliorer l'échange d'informations entre eux et de travailler à l'accomplissement de la mission de développement, à la coopération et à l'échange d'expertise. Entre le 3 et le 7 juillet 2023, la réunion plénière s'est tenue à Abu Dhabi, aux Émirats arabes unis, et a rassemblé 533 délégués, douze observateurs et un partenaire international. Une étape importante a été franchie avec la décision de passer à une nouvelle infrastructure informatique, l'Egmont Secure Web. L'infrastructure informatique

a été un point de mire important de la réunion plénière : les communications de soupçons et les demandes de l'étranger, en forte augmentation, ne peuvent plus être gérées uniquement avec de la main-d'œuvre. Les CRF ont besoin de nouvelles solutions informatiques pour améliorer leur efficacité.

7.2 GAFI

Le GAFI est une organisation intergouvernementale créée par le G7 lors d'une réunion ministérielle qui s'est tenue à Paris en 1989. Il est le principal organisme international de lutte contre le blanchiment d'argent ainsi que le financement du terrorisme et de la prolifération. Ses membres sont les pays respectifs, et non des offices individuels. Il enquête sur la manière dont l'argent est blanchi et le terrorisme financé. Il promeut des normes mondiales⁷⁹ visant à réduire les risques et évalue si les pays prennent des mesures efficaces.

En 2023, trois réunions plénières présidées par Singapour se sont tenues au siège de l'Organisation de coopération et de développement économiques, à Paris⁸⁰.

Le GAFI a publié quelques rapports en 2023 (en anglais uniquement), notamment sur l'utilisation abusive de la citoyenneté et du domicile par le biais de programmes d'investissement⁸¹, les meilleures pratiques pour lutter contre l'utilisation abusive des organisations à but non lucratif⁸² les flux financiers illicites issus de la cyber-escroquerie⁸³ et le financement participatif destiné au financement du terrorisme⁸⁴. Ce dernier en particulier a gagné en actualité du fait des attaques terroristes du Hamas contre Israël commises le 7 octobre 2023. À ce propos, le MROS a envoyé le 3 novembre 2023 un courrier de sensibilisation

⁷⁸ Le groupe régional Egmont II comprend notamment aussi le Financial Crimes Investigation Board (MASAK) de Turquie, le State Financial Monitoring Service of Ukraine (SFMS) et la UK Financial Intelligence Unit (UKFIU) du Royaume-Uni.

⁷⁹ *Recommendations du GAFI – 2012*, mise à jour en novembre 2023.

⁸⁰ La décision de suspendre la Russie prise lors de la première réunion en février 2023 est remarquable à cet égard : *FATF Statement on the Russian Federation*.

⁸¹ *Misuse of Citizenship and Residency by Investment Programmes*.

⁸² *Best Practices on Combating the Abuse of Non-Profit Organisations*.

⁸³ *Illicit Financial Flows from Cyber-enabled Fraud*.

⁸⁴ *Crowdfunding for Terrorism Financing*.

(alerte) et une liste de typologies aux IF suisses; il a complété l'alerte le 5 décembre 2023 par un addendum⁸⁵.

Évaluation mutuelle

Le GAFI établit des normes visant à évaluer les mesures de lutte contre le blanchiment d'argent et le financement du terrorisme, qui s'appliquent aux pays membres tenus de mettre en œuvre ces mesures. Il évalue périodiquement leur mise en œuvre dans ces différents pays et publie ses résultats dans un rapport. Ses recommandations ne sont pas juridiquement contraignantes, mais elles sont d'une grande importance pour la Suisse. Les pays membres qui présentent des lacunes importantes par rapport à ces recommandations sont désignés publiquement et placés sur une liste de pays à risque (liste grise ou liste noire), ce qui a généralement des conséquences importantes pour eux. Les transactions en provenance ou à destination de ces pays sont soumises à un contrôle officiel, ce qui les rend plus lourdes et plus coûteuses. Les investisseurs étrangers se tiennent en outre à l'écart, car le risque leur semble trop grand. La réputation de toute leur place financière en pâtit alors. La Suisse a été soumise pour la dernière fois à une évaluation mutuelle en 2016, lors du quatrième cycle d'évaluation. Si le résultat a été positif, son dispositif de défense présente toutefois certaines lacunes, raison pour laquelle la Suisse a fait l'objet d'un suivi dit renforcé. Pour se conformer aux recommandations du GAFI, elle a systématiquement mis en œuvre différentes mesures visant à améliorer sa conformité technique, notamment en révisant la LBA en juillet 2021⁸⁶. Le GAFI a entre-temps reconnu ses progrès et la Suisse a pu réintégrer le processus de suivi régulier en octobre 2023. La prochaine évaluation mutuelle est prévue pour 2027–2028. Le GAFI réévaluera le dispositif de la Suisse de manière globale au moyen d'une

méthodologie nouvelle par rapport à 2016. Outre le respect technique des normes du GAFI, un accent supplémentaire sera désormais mis sur l'efficacité du dispositif de défense. L'évaluation ne portera pas seulement sur les autorités de la Suisse, mais sur l'ensemble de sa place financière, y compris le secteur privé. Le GAFI vérifie en effet si les pays connaissent leurs risques et ont pris des mesures pour les limiter, voire les éliminer.

La nouvelle méthodologie comprend deux volets interdépendants :

- le volet **conformité technique** évalue si les mesures requises par les différentes recommandations du GAFI sont appliquées et porte principalement sur le cadre juridique et institutionnel du pays, ainsi que sur les pouvoirs et les procédures des autorités compétentes. Ce sont là les éléments fondamentaux d'un système efficace de lutte contre le blanchiment d'argent et le financement du terrorisme et de la prolifération⁸⁷;
- le volet **efficacité** évalue la mesure dans laquelle un pays garantit un système robuste de lutte contre le blanchiment d'argent et le financement du terrorisme. Il analyse en outre dans quelle mesure le cadre juridique et institutionnel d'un pays influe sur les résultats attendus⁸⁸.

L'évaluation mutuelle dure environ 18 mois et peut être divisée en trois phases pour la Suisse : la préparation de la visite sur place (à partir de 2024), la visite sur place (vers juillet 2027) et la préparation à la réunion plénière du GAFI, au cours de laquelle le rapport sur la Suisse sera adopté.

⁸⁵ L'alerte du MROS comprenait des publications de la GAFI ainsi que des informations de CRF étrangères et des renseignements propres au MROS.

⁸⁶ Notamment par l'introduction d'une nouvelle compétence de clarification du MROS en vertu de l'art. 11a, al. 2^{bis} LBA.

⁸⁷ Le niveau de conformité aux différentes recommandations est indiqué par l'une des évaluations suivantes : conforme, largement conforme, partiellement conforme ou non conforme.

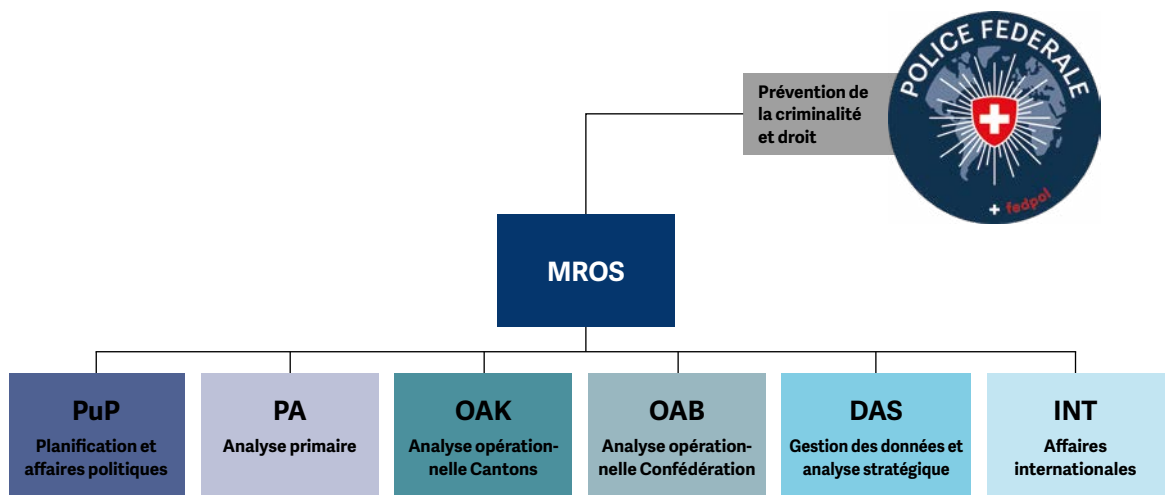
⁸⁸ Le niveau d'efficacité est évalué comme suit : élevé, considérable, modéré ou faible.

8. 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.

Il a été réorganisé en 2020 et comprend depuis lors six domaines (cf. organigramme de la Fig. 17). En 2023, il employait environ 59 collaborateurs (50,3 équivalents temps plein).

Fig. 17: Organisation du MROS



Planification et affaires politiques (PuP)

Le domaine PuP fonctionne comme une discipline transversale classique. Il se concentre sur les questions juridiques relevant du blanchiment d'argent et du financement du terrorisme, sur le traitement et le suivi des projets politiques et des publications (par ex. rapports annuels, révisions de lois, avis de droit sur des thèmes techniques spécifiques au MROS) et apporte un soutien aux domaines opérationnels du MROS. Il entre-

tient des échanges réguliers avec les parties prenantes internes et externes et s'occupe des questions administratives du MROS.

Analyse primaire (PA)

Le Domaine PA est responsable de l'enregistrement et de la préparation de toutes les communications entrantes du point de vue formel, technique et matériel. Il est aussi chargé des corrections manuelles lorsque la qualité des données n'est

pas satisfaisante. Par ailleurs, il prend en charge le tri des cas et les transmet à un des domaines en aval sur la base d'une évaluation globale. Il est aussi compétent pour l'entraide administrative nationale au sens de l'art. 29 LBA.

Analyse opérationnelle Cantons (OAK)

Le Domaine OAK analyse les communications de soupçons entrantes qui relèvent en majorité de la compétence des autorités de poursuite pénale cantonales et lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées aux autorités de poursuite pénale compétentes, soit en général celles des cantons. Si nécessaire, il partage les informations avec d'autres autorités nationales ainsi qu'avec des CRF d'autres pays.

Analyse opérationnelle Confédération (OAB)

Le Domaine OAB analyse les communications de soupçons entrantes qui relèvent a priori du MPC et lui ont été attribuées par le Domaine PA. En cas de soupçon fondé, il transmet les informations agrégées aux autorités de poursuite pénale compétentes, soit en général le MPC ou celles des cantons. Si nécessaire, il partage les informations avec d'autres autorités nationales ainsi qu'avec des CRF de l'étranger.

Gestion des données et analyse stratégique (DSA)

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

Affaires internationales (INT)

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

