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

Rapport annuel 2020

Mai 2021

Bureau de communication en matière de blanchiment d'argent

Rapport annuel 2020

Mai 2021

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) 058 463 40 40
E-Mail : mros.info@fedpol.admin.ch

Internet : http://www.fedpol.admin.ch

Table des matières

1. Avant-propos

L'année 2020 a constitué une fois de plus un défi pour le Bureau de communication en matière de blanchiment d'argent (MROS). La situation exceptionnelle découlant de la pandémie provoquée par le COVID-19 a pu être maîtrisée du fait de l'introduction du système de communication électronique goAML. Mais la pandémie a aussi offert aux criminels plusieurs opportunités d'enrichissement illégal, augmentant ainsi les risques de blanchiment d'argent. Ce risque s'est matérialisé par une nouvelle hausse du nombre de communications de soupçons effectuées au MROS. Les 5334 communications reçues en 2020 portaient sur plus de 9000 relations d'affaires, un chiffre supérieur de quelque 25 % à celui de 2019. Le taux de croissance du nombre de communications de soupçons effectuées au MROS est donc pour 2020 du même ordre que celui des années 2018 et 2019. Durant l'année écoulée, le MROS a par ailleurs traité plus de 6000 relations d'affaires signalées depuis 2016, dont l'analyse était en cours à la fin de l'année 2019.

Plus de 1000 signalements effectués en 2020 concernaient des soupçons d'escroquerie en relation avec les crédits accordés par les institutions financières sous le cautionnement de la Confédération. Ils ont amené le MROS à effectuer plus de 800 dénonciations aux autorités de poursuite pénale. Des centaines d'instructions pénales ont été ouvertes. Cette particularité se reflète dans les statistiques. L'escroquerie est ainsi mentionnée comme infraction préalable dans plus de la moitié des communications effectuées au MROS en 2020 (58 %), une hausse notable par rapport à 2019 (25 %). Pour la première fois, pendant l'année sous revue, la surveillance des transactions est l'élément le plus souvent mentionné comme étant à l'origine des soupçons des intermédiaires financiers.

Le système goAML s'est imposé auprès des intermédiaires financiers. En décembre 2020, près de 90 % des communications effectuées au Bureau de communication étaient transmises par voie électronique. Ce résultat encourageant résulte des efforts importants entrepris par les intermédiaires financiers pour s'adapter à ce nouveau système. Pour sa part, le MROS a consacré des ressources substantielles pour soutenir et accompagner les intermédiaires financiers et les autorités dans cette transition. Toutefois, les données transmises nécessitent parfois encore un travail de correction et de toilettage conséquent de la part du Bureau de communication pour permettre leur analyse. Les ressources substantielles que le MROS a dû y consacrer en 2020 doivent à l'avenir être dédiées à l'analyse. Des améliorations et des adaptations doivent donc être entreprises afin d'utiliser pleinement le potentiel offert par les communications électroniques.

Pour la première fois, le MROS présente dans son rapport annuel des typologies thématiques destinées à attirer l'attention des intermédiaires financiers sur les risques de blanchiment d'argent, du crime organisé ou de financement du terrorisme dont la détection est difficile. Nous avons choisi de mettre en lumière des typologies spécifiques relatives aux risques de financement du terrorisme, de participation à une organisation crimi-

nelle, de traite d'êtres humains et de blanchiment d'argent entrepris au moyen de crypto-monnaies ou d'identification en ligne. Le développement de l'analyse stratégique et la sensibilisation des intermédiaires financiers sont des objectifs centraux de la nouvelle stratégie du Bureau de communication. Le traitement électronique des communications de soupçons offre à cet égard de nouvelles possibilités que le MROS exploitera davantage encore dans les années à venir.

Autre nouveauté, le MROS présente cette année des statistiques consolidées sur l'échange d'informations effectué avec les autorités nationales. Ces échanges ont en effet acquis une importance nouvelle, à la fois du point de vue de leur contenu et de la charge qu'ils représentent pour le MROS. Les échanges avec les homologues étrangers ont connu eux aussi une nouvelle hausse durant l'année sous revue. En septembre 2020, le législateur a adopté une modification de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA)[1] octroyant au MROS des compétences accrues dans ce domaine. À l'avenir, le MROS pourra solliciter auprès des intermédiaires financiers – aux conditions d'un nouvel art. 11a, al. 2bis, LBA – des renseignements sur des relations d'affaires faisant l'objet d'informations provenant uniquement d'un homologue étranger. Ces améliorations contribueront à renforcer l'efficacité du dispositif anti-blanchiment helvétique.

Le MROS n'aurait pu obtenir ces résultats sans les efforts de ses collaboratrices et collaborateurs, à qui nous tenons à exprimer notre reconnaissance et nos remerciements.

Berne, mai 2021

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

Bureau de communication en matière de blanchiment d'argent MROS

[1] RS **955.0**

2. Nouvelle organisation et stratégie 2020-2021 du MROS

Pour le MROS, 2020 a marqué un tournant. L'année a été caractérisée par le changement et la nouveauté. Le 1er janvier 2020, goAML, le système d'information du MROS, est entré en fonction, accompagné d'une version révisée de l'ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent (OBCBA)[2]. Le même jour, le MROS se dotait d'une nouvelle stratégie qui est complémentaire à la stratégie de lutte contre la criminalité 2020-2023 du Département fédéral de justice et police (DFJP).[3] Ces transformations se reflétaient enfin dans une réorganisation interne du MROS, destinée à assurer l'utilisation de goAML et la mise en œuvre de cette stratégie (cf. ch. 2.3). Ces évolutions interdépendantes procèdent de la volonté de transformer le MROS et d'en faire une autorité moderne, proactive, capable de relever les défis posés par l'évolution constante des techniques de blanchiment d'argent et ses infractions préalables, de la criminalité organisée ou de financement du terrorisme.

2.1 Une décennie d'évolutions dans le domaine de la lutte contre le blanchiment d'argent, la criminalité organisée et le financement du terrorisme

Entre 2010 et 2019, le nombre de relations d'affaires signalées par les intermédiaires financiers helvétiques au MROS par an a été multiplié par sept. Les échanges d'informations avec des cellules de renseignements financiers (CRF) étrangères ont augmenté et le MROS a été sollicité toujours davantage par des autorités nationales dans le cadre de l'entraide administrative. Ces tendances se sont poursuivies au cours de l'année sous revue (cf. ch. 4). Rien n'indique qu'elles s'inverseront. Depuis 2013, le MROS a été doté de compétences supplémentaires, notamment dans le domaine de l'échange d'informations avec ses homologues étrangers et avec les intermédiaires financiers.[4] Celles-ci sont amenées à s'étendre à nouveau à partir du 1er juillet de cette année (cf. ch. 6.2).

À des rythmes et à des degrés divers, de nombreuses CRF ont été confrontées à des évolutions analogues. Le volume d'informations financières qu'elles reçoivent croît ; les techniques de blanchiment d'argent ont évolué, notamment en relation avec l'usage de nouvelles technologies (cf. ch. 5.5); le rôle des CRF dans le dispositif anti-blanchiment gagne en importance ; leurs compétences s'étoffent, en particulier sous l'angle de l'échange d'information national et international. L'amélioration globale des dispositifs de lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée et le financement du terrorisme se lit derrière ces évolutions : les signaux qu'ils produisent sont plus nombreux, mais tous ne sont pas pertinents pour les autorités de poursuite pénale. Le rôle de filtre des CRF est crucial.

---

2 RS **955.23**

3 Cf. *stratégie du DFJP de lutte contre la criminalité 2020-2023.*

4 À ce sujet, voir le *rapport annuel 2013 du MROS*, pp. 56 ss, sur la page internet du MROS.

Le paradigme dans lequel les CRF opèrent s'est modifié sur le plan international. Voici plus de vingt ans, lors de l'émergence des standards internationaux en matière de blanchiment d'argent, l'identification et la saisie des valeurs patrimoniales provenant d'un crime étaient la finalité du dispositif légal. Une vocation préventive s'ajoute désormais à cet objectif répressif. Le rôle dévolu aux CRF a évolué en conséquence : leur mission ne consiste pas seulement à identifier les informations utiles aux autorités de poursuite pénale, mais aussi à utiliser l'ensemble des signaux renvoyés par le dispositif de lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée et le financement du terrorisme pour en identifier les points faibles. À cette fin, les CRF produisent des analyses stratégiques destinées à identifier les méthodes et les tendances dans ces domaines, et partagent leurs constats avec les intermédiaires financiers, les négociants, les autorités tierces, les décideurs ou le public intéressé (*follow the money*).
Durant la décennie écoulée, les ressources du MROS ont augmenté, mais à un rythme insuffisant pour que le bureau de communication puisse continuer à assumer ses fonctions avec les méthodes existantes. Les changements intervenus au début de l'année 2020 procèdent de la volonté de refléter les évolutions de la décennie passée afin de mieux relever les défis futurs. L'introduction de goAML, un système informatique capable d'assurer le traitement informatisé des informations signalées au MROS, est la pierre angulaire de cette stratégie. Ce système permet de communiquer de façon rapide et sécurisée avec les intermédiaires financiers et les autorités nationales. Il permet aussi aux analystes du MROS de traiter les informations reçues en s'épargnant un fastidieux travail de saisie. Au-delà des gains d'efficacité, ce pas vers la numérisation n'est qu'une étape vers l'usage accru de techniques d'analyse recourant à l'intelligence artificielle et permettant l'analyse de volumes de données importants (*intelligence led policing*). Nous effectuons plus bas un premier bilan de l'usage de goAML, un an après son introduction (cf. ch. 3).

2.2 La stratégie 2020-2021 du MROS

Avec effet au début de 2020, le MROS a adopté une nouvelle stratégie pour les années 2020-2021. Celle-ci s'articule autour de sept axes interdépendants :

1) Les analyses du MROS sont effectives
2) La qualité des communications est améliorée
3) Le MROS renforce la prévention des formes de criminalité les plus graves
4) Les autorités de poursuite pénale sont soutenues de façon optimale
5) La collaboration internationale est renforcée et effective
6) Les capacités techniques du MROS sont développées
7) Les collaborateurs du MROS approfondissent leurs connaissances et les mettent régulièrement à jour

Le premier objectif de cette stratégie consiste à traiter plus effectivement les informations qui parviennent au MROS. Ceci suppose un tri rapide, permettant de déterminer de façon adéquate le type d'analyse requis, afin d'engager les ressources du MROS là où elles génèrent le plus de valeur ajoutée. À terme, ce tri doit être lui aussi soutenu par des outils d'intelligence artificielle, qui repèrent rapidement les éléments saillants d'une communication de soupçons, ou leur rapport avec des affaires en cours, par exemple. Depuis le 1er janvier 2020, la profondeur de l'analyse du MROS – comme le nombre et le type de vérifications effectuées par les collaborateurs – est déterminée en fonction de ce tri. Elle dépend d'une part des éléments caractérisant la communication (par exemple la complexité des opérations signalées), d'autre part de la stratégie de lutte contre la criminalité 2020-2023 du DFJP et des besoins des autorités de poursuite pénale. Elle est déterminée selon des critères de priorisation internes.
Depuis le 1er janvier 2020, des efforts importants ont été consentis pour que l'analyse corresponde au mieux aux besoins des autorités de poursuite pénale. Des échanges réguliers ont eu lieu à ce sujet avec les partenaires du MROS. Le nouveau système d'information permet de livrer

des informations provenant des communications de soupçons de manière informatisée. Par ailleurs, les cas de peu d'importance sont traités rapidement, et les processus internes du MROS ont été reconfigurés afin de mobiliser moins de ressources.
Le second objectif de cette stratégie vise à renforcer le rôle joué par le MROS dans la dimension préventive évoquée plus haut. Il s'agit ici de renforcer l'analyse stratégique consacrée aux risques, tendances et méthodes de blanchiment d'argent ou de financement du terrorisme, et d'en partager les constats avec les intermédiaires financiers, les négociants ou avec les autorités concernées, par exemple dans le cadre du processus d'évaluation nationale des risques effectué sous l'égide du Groupe de coordination interdépartemental sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF). Ces travaux se poursuivront en 2021.
La mise en œuvre de cette stratégie suppose des échanges plus étroits entre le MROS et ses partenaires, qu'il s'agisse des autorités nationales ou internationales, des organisations internationales – en premier lieu, le Groupe d'action financière (GAFI) et le groupe Egmont –, ou du secteur privé. La qualité des informations échangées avec les homologues étrangers doit être développée et les nouvelles compétences du MROS y contribueront. La collaboration avec les intermédiaires financiers doit être institutionnalisée par un partenariat public-privé permettant aux intermédiaires financiers de mieux détecter les risques ainsi que les opérations suspectes, d'effectuer des communications de soupçons de qualité et d'agir de façon préventive (*public private partnership*).

2.3 La nouvelle organisation du MROS

En 2019, le Conseil fédéral a doté le MROS de douze postes à plein temps supplémentaires. Au 31 décembre 2020, le MROS disposait de 57 postes occupés pour un total de 48,8 équivalents plein temps, dont 10,3 équivalents plein temps engagés avec des contrats à durée déterminée.
La mise en œuvre de la stratégie 2020-2021 du MROS rendait nécessaire la réorganisation de cette division de fedpol. Depuis le 1er janvier 2020, le MROS est donc subdivisé en six domaines, disposant chacun de tâches spécifiques. Trois domaines sont responsables de l'analyse opérationnelle, c'est-à-dire principalement du traitement des communications de soupçons effectuées au MROS. Parmi eux, le domaine « analyse préliminaire » est responsable de la réception des informations reçues et a un rôle de coordination pour le tri et l'attribution des communications. Il traite également les cas qui nécessitent une analyse rapide. Les deux autres domaines s'occupent de l'analyse approfondie, l'une pour les cas de compétence cantonale (« analyse opérationnelle Cantons »), l'autre pour les cas de compétence fédérale (« analyse opérationnelle Confédération »). Ensuite, un quatrième domaine s'occupe de l'échange international d'informations et se charge également des travaux liés à la participation du MROS aux activités des organisations internationales (GAFI, groupe Egmont). Enfin, le domaine « analyse stratégique » explore les méthodes et les tendances de blanchiment d'argent et effectue les tâches relatives à l'analyse nationale des risques dévolues au MROS, tandis que le domaine « planification et affaires politiques » se charge des tâches de conduite de la division, des échanges avec d'autres autorités nationales et des processus juridiques impliquant le Bureau de communication.

2.4 Les défis à venir

L'année 2020 a été intense pour le MROS. Durant les premiers mois de l'année, la priorité a été donnée à la mise en œuvre du nouveau système de communication électronique. Ce choix s'est révélé judicieux, dans la mesure où goAML a permis au Bureau de communication d'assumer ses tâches en dépit des circonstances extraordinaires créées par la pandémie dès le mois de mars. Toutefois, l'introduction de ce système a nécessité plusieurs adaptations et les défis qui en résultent ne sont pas tous résolus, notamment sous l'angle de la qualité des informations transmises par les intermédiaires financiers et les négociants. Ce chantier reste prioritaire pour le MROS. Il suppose initialement des efforts importants, mais à terme, la durée de traitement des communications de soupçons sera réduite et

la qualité de l'analyse s'en trouvera renforcée. Durant l'année 2020, le MROS a en outre traité les plus de 6000 relations d'affaires signalées durant la période 2016-2019 qui étaient encore en cours d'analyse à la fin de l'année 2019 (cf. ch. 4.13). En 2021, les priorités du MROS seront centrées sur la mise en œuvre de sa stratégie. Le travail d'analyse stratégique sera renforcé et l'échange avec les intermédiaires financiers développé.

3. Introduction du nouveau système d'information goAML au MROS

Le 1er janvier 2020, le MROS a introduit le nouveau système d'information goAML. Ce changement de système est une étape indispensable vers la numérisation. goAML permet aux intermédiaires financiers, aux négociants, ainsi qu'aux autorités et organisations (organismes d'autorégulation [OAR] et organismes de surveillance [OS]) soumis à la LBA, d'effectuer leurs communications de soupçons de façon électronique via un portail en ligne. Ce système permet aussi au MROS de transmettre sur la base de l'art. 23, al. 4, LBA ses rapports d'analyse ainsi que les informations et documents qui les accompagnent aux autorités de poursuite pénale suisses compétentes – ainsi qu'échanger des informations avec des autorités suisses aux conditions de l'art. 29 LBA – par voie électronique.
En quelques mois, le système goAML s'est établi comme un outil indispensable, assurant une communication sécurisée et efficace entre le MROS et ses interlocuteurs. La transmission et le traitement électroniques des communications de soupçons ont considérablement réduit la consommation de papier du MROS, mais surtout, les possibilités de télétravail offertes par le nouveau système se sont avérées très utiles dans les circonstances générées par la pandémie.
Néanmoins, ce système a confronté le MROS à certains défis en matière de transmission des données. Le 21 juillet 2020, le MROS a annoncé aux intermédiaires financiers que seules les transactions suspectes en vertu de l'art. 3, al. 1, let. h, OBCBA devaient désormais être signalées électroniquement au MROS. Un délai fixé au 1er avril 2021 permettait aux intermédiaires financiers d'adapter leur pratique.[5]
En outre, la qualité des données transmises par les intermédiaires financiers est parfois insuffisante (cf. ci-après, ch. 3.5).

3.1 Nombre d'intermédiaires financiers enregistrés

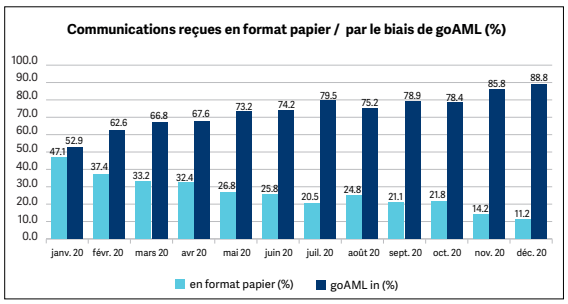
Au 31 décembre 2020, 728 intermédiaires financiers s'étaient enregistrés dans goAML, créant des comptes pour un total de 1494 utilisateurs. Certains intermédiaires financiers ont débuté une procédure d'enregistrement, sans toutefois l'achever.
Seuls 252 des 728 intermédiaires financiers enregistrés dans goAML ont effectivement transmis une communication de soupçons au MROS via goAML en 2020.

3.2 Part de communications de soupçons effectuées par voie électronique

Depuis l'introduction de goAML, les intermédiaires financiers ont largement fait usage de la possibilité d'effectuer des communications de soupçons électroniques. La proportion de communications effectuées via goAML dépassait déjà 50 % en janvier et a crû au cours des mois suivants pour atteindre presque 90 % en

[5] Cf. publication *Adaptations de la pratique relative aux communications via goAML sur le site Internet du MROS.* Cette publication a été remplacée par la version 2.0, en date du 30 mars 2021 *(Adaptation de la pratique pour les communications via goAML valable dès le 01.04.2021).*

décembre 2020. Le graphique suivant montre l'évolution de la proportion de communications reçues sous forme papier et via goAML durant l'année 2020 :



Le système goAML a également fait ses preuves au cours de l'année 2020 sous l'angle des demandes d'informations du MROS fondées sur l'art. 11a LBA. Les intermédiaires financiers peuvent en effet aussi utiliser goAML pour répondre à de telles demandes. Dans ce domaine également, les intermédiaires financiers ont fait un usage croissant du nouveau système de communication électronique. La proportion des réponses effectuées par voie électronique a en effet augmenté de 46 % en janvier à 68 % en décembre 2020. Le MROS espère que cette croissance se poursuivra en 2021.

3.3 Variantes permettant d'effectuer des communications de soupçons via goAML

Diverses solutions techniques ont été développées afin de répondre le mieux possible aux besoins des intermédiaires financiers souhaitant effectuer leurs communications de soupçons au MROS par voie électronique. Trois variantes différentes sont à leur disposition (cf. ci-dessous). Des informations et documents complémentaires sur ces variantes sont disponibles en ligne.[6]

3.3.1 Saisie automatique des données (téléchargement)

L'intermédiaire financier souhaitant effectuer une communication en utilisant la variante automatique doit d'abord installer une application lui permettant d'exporter les données se trouvant dans son système informatique vers un fichier XML établi selon une structure prédéfinie. Le fichier ainsi généré est ensuite téléchargé sur le portail en ligne de goAML, puis transmis au MROS. Le développement de l'application nécessaire incombe à l'intermédiaire financier.

3.3.2 Saisie semi-automatique

La variante semi-automatique consiste à effectuer une saisie manuelle des informations générales relatives à la communication de soupçon sur le portail en ligne de goAML, puis à compléter celles-ci en téléchargeant un fichier XML contenant les informations relatives aux comptes et aux transactions qu'il choisit de signaler au MROS. Ces informations peuvent ensuite être complétées manuellement. Cette fonctionnalité permet aux intermédiaires financiers qui ne souhaitent pas recourir à la solution automatique, mais qui ont néanmoins un nombre important de transactions à signaler d'économiser du temps. L'usage de cette variante suppose que les transactions issues du système bancaire de l'intermédiaire financier soient d'abord enregistrées localement dans un fichier XML disposant d'un format structuré prédéfini. Ce fichier est destiné à être ensuite importé dans goAML.

3.3.3 Saisie manuelle

La variante manuelle suppose la saisie de données, effectuée directement sur le portail en ligne goAML. Elle ne présente aucune difficulté technique ; l'utilisateur doit disposer d'un accès à Internet et de ses données de connexion personnelles. Il doit saisir les informations constituant sa communication de soupçons en remplissant les différents champs d'un formulaire en ligne. Selon la nature de la communication de soupçons, cette saisie manuelle peut prendre un certain temps. C'est en particulier le cas lorsque les données de nombreuses transactions doivent être saisies.

[6] Cf. *Informations concernant l'introduction du nouveau système de traitement des données goAML au MROS* sur le site Internet du MROS.

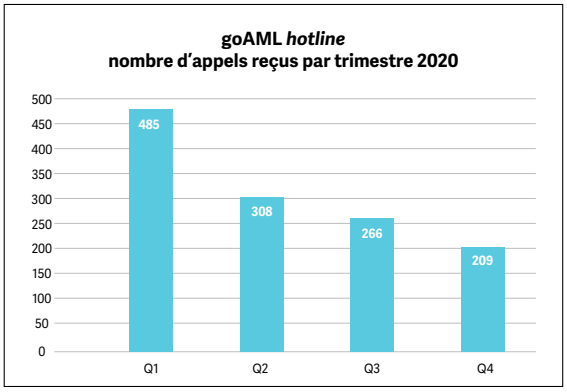
3.4 Assistance aux utilisateurs de goAML

Lors de l'introduction de goAML, le MROS a publié sur internet une marche à suivre pour la saisie manuelle de communications sur le portail en ligne. Au cours de l'année 2020, le MROS a régulièrement actualisé un document présentant des réponses aux questions fréquemment posées par les intermédiaires financiers[7], et adapté le manuel destiné aux utilisateurs de goAML.[8] D'autres documents destinés à assister les intermédiaires financiers lors de la saisie de leurs communications de soupçons ont également été publiés en ligne. Une newsletter livrant des conseils et des astuces aux intermédiaires financiers enregistrés dans goAML a également été envoyée. De telles lettres d'information permettent d'atteindre directement les utilisateurs de goAML de façon commode. Le MROS prévoit d'en envoyer régulièrement.

3.4.1 *Hotline* goAML

Afin d'assister le mieux possible les intermédiaires financiers, les autorités et d'autres utilisateurs dans leur transition vers goAML, le MROS a installé une *hotline* goAML (téléphone ou e-mail). Les collaborateurs du MROS ont assuré le service de celle-ci, en offrant un important support technique (par ex. pour l'enregistrement en cas de questions spécifiques sur la saisie d'une communication ou sur la procédure de communication automatique par fichier XML). Durant le premier semestre 2020, pendant lequel de nombreux intermédiaires financiers ont dû s'enregistrer dans le nouveau système, plusieurs dizaines de personnes ont recouru à la *hotline* goAML chaque jour. Aujourd'hui, le système d'information goAML est bien accepté par un grand nombre d'intermédiaires financiers. Leurs retours positifs montrent que les efforts consentis par le MROS ont porté leurs fruits, même s'ils ont impliqué une charge de travail supplémentaire importante.

Le graphique ci-dessous donne un aperçu de l'utilisation de la *hotline* goAML en 2020. Au total, les collaborateurs de la *hotline* du MROS ont reçu 1268 appels et ont répondu à de nombreux autres appels sur leurs numéros de téléphone directs (par ex. lorsqu'une question d'un intermédiaire financier impliquait un travail de suivi et des contacts ultérieurs).



3.5 Qualité des informations transmises par les intermédiaires financiers

Dès l'introduction de goAML, le MROS a constaté que la qualité des données transmises par les intermédiaires financiers était parfois insuffisante, en particuliers les informations relatives aux transactions. Le MROS a dû consacrer beaucoup de temps à corriger, saisir et toiletter ces données pour pouvoir effectuer ses analyses sur une base solide. Ce travail a été effectué en grande partie manuellement. Il n'était par exemple pas toujours possible de déterminer clairement quelle personne ou quelle relation d'affaires faisait l'objet de la communication. En outre, le MROS s'est engagé à expliquer aux intermédiaires financiers les erreurs systémiques résultant de la programmation de leurs interfaces, afin de diminuer le nombre de communications rejetées automatiquement du fait d'une qualité insuffisante des données.
Le MROS et les autorités de poursuite pénale doivent pouvoir compter sur des données de bonne qualité. Il faut éviter à tout prix que le

[7] f. publication *goAML : Frequently Asked Questions (FAQ)* sur le site Internet du MROS.

[8] Cf. publication *goAML-Web – Manuel d'utilisation,* sur le site Internet du MROS.

MROS doive systématiquement corriger et compléter des données incorrectes, ce qui annulerait l'un des principaux avantages du système de communication électronique.
Il importe que les données livrées par les intermédiaires financiers soient correctes et exploitables, afin que le MROS et les autorités de poursuite pénale compétentes puissent les analyser de manière efficace et ciblée. Lorsqu'il s'agit de communiquer des transactions, il est indispensable que les informations nécessaires de base (renseignements sur les personnes, les comptes, etc.) permettent aux autorités précitées de faire leur travail d'analyse.

3.6 Perspectives

L'Office des Nations Unies contre la drogue et le crime (ONUDC), une division de l'organisation des Nations Unies (ONU) à Vienne, fournit le logiciel goAML. Ce dernier est déjà utilisé dans plus de 60 pays. L'ONUDC continue de développer ce logiciel en permanence. De nouvelles fonctionnalités sont développées, notamment au sujet des crypto-monnaies, des relations *entity-to-entity* et des personnes politiquement exposées (PPE). Ces améliorations sont effectuées en étroite collaboration avec les CRF concernées et en fonction de leurs souhaits. Une nouvelle version de goAML est en préparation.

4. Statistique annuelle du Bureau de communication

La façon de compter les communications des soupçons reçues par le MROS a été adaptée avec l'introduction de goAML. Depuis le 1er janvier 2020, le chiffre des communications de soupçons effectuées au MROS est celui des communications effectuées par les intermédiaires financiers et non plus, comme auparavant, celui du nombre de relations d'affaires signalées. Comme plusieurs relations d'affaires peuvent être signalées au sein de la même communication, des comparaisons exactes avec les chiffres des années précédentes s'avèrent difficiles.

Pour donner néanmoins une idée de la progression chronologique des statistiques, nous avons choisi de publier, à chaque fois que c'était possible, des chiffres sous la forme de pourcentages. Pendant l'exercice 2019, chaque communication au MROS par les intermédiaires financiers suisses comprenait en moyenne 1,8 relation d'affaires. Nous avons retenu ce taux moyen pour évaluer la progression des communications reçues par le MROS en 2020 et effectuer des comparaisons avec les chiffres des années précédentes là où c'était possible.

4.1 Tableau récapitulatif du MROS 2020

Résumé de l'exercice 2020
(1er janvier 2020-31 décembre 2020)

Nombre de communications	2020 Absolu	2020 Relatif
Total des communications reçues	**5 334**	**100,0 %**
Communications traitées	4 505	84,5 %
Communications en cours d'analyse au 31 décembre 2020	829	15,5 %
Type d'intermédiaire financier		
Banques	4 773	89,5 %
Prestataires de services de paiement	185	3,5 %
Autres	121	2,3 %
Cartes de crédit	83	1,6 %
Gérants de fortune / Conseillers en placement	45	0,9 %
Fiduciaires	30	0,6 %
Maisons de jeu	29	0,5 %
Assurances	20	0,4 %
Opérations de crédit, de leasing, d'affacturage et de financement à forfait	19	0,4 %
Négociants en matières premières et métaux précieux	12	0,2 %
Avocats et notaires	6	0,1 %
Trustees	4	0,1 %
Bureaux de change	3	0,1 %
Négociants en valeurs mobilières	2	0,0 %
Organisme d'autorégulation (OAR)/ FINMA/CFMJ	2	0,0 %

Ce tableau donne un aperçu des communications reçues par le MROS pendant l'année sous revue, mais pas de la totalité des communica-

tions traitées en 2020. À la fin de 2019, 6095 relations d'affaires annoncées entre 2016 et 2019 étaient encore en cours de traitement. Pour l'essentiel, ces relations d'affaires ont pu être traitées pendant l'année sous revue (cf. ci-après, ch. 4.13). Ces communications n'apparaissent pas dans le tableau ci-dessus.

Dénonciations	1939	100,0 %
Au Ministère public de la Confédération	175	9,0 %
Aux ministères publics cantonaux	1764	91,0 %

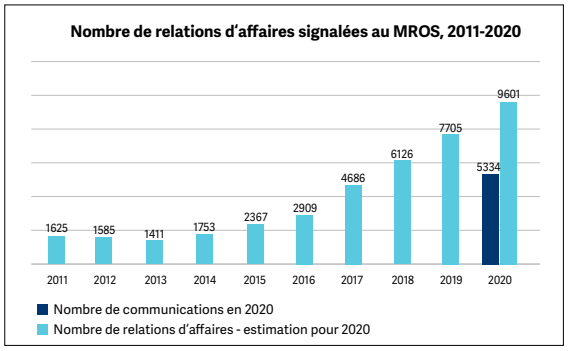
Le tableau ci-dessus donne un aperçu des dénonciations effectuées en 2020 par le MROS aux autorités de poursuite pénale. Contrairement à ce qui prévalait jusqu'en 2019, les dénonciations ne consistent plus en la transmission, après analyse, des communications reçues par le MROS. Elles consistent en des rapports élaborés par le MROS sur la base des informations à sa disposition, dont les communications sont la source principale, mais non la seule. Les informations contenues dans une dénonciation peuvent ainsi être tirées de sources provenant de différentes autorités et de plusieurs communications (cf. ci-après, ch. 4.12). Dans une minorité de cas, les dénonciations effectuées en 2020 contenaient des informations communiquées pendant les années précédentes, de sorte que le nombre de dénonciations effectuées pendant l'année sous revue ne peut pas être rapporté au nombre de communications reçues pendant la même période.

4.2 Constatations générales

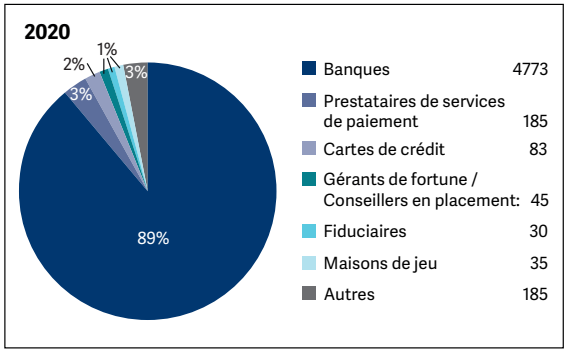
1. En 2019, 7705 relations d'affaires ont été communiquées au MROS. En revanche en 2020, le bureau de communication a reçu 5334 communications de soupçons. En fonction du chiffre moyen de relations d'affaires par communication soumises au MROS par les intermédiaires financiers suisses en 2019 – lequel s'élève à 1,8 relation d'affaires par communication – on peut estimer que les 5334 communications reçues par le MROS en 2020 correspondent à une augmentation d'environ 25 % des relations d'affaires signalées par rapport à l'exercice précédent.
2. Cette augmentation s'explique en partie par la réception de nombreuses communications adressées au MROS pour des soupçons de détournement ou d'obtention frauduleuse de crédits COVID.
3. Les banques continuent de représenter le secteur d'intermédiation financière à l'origine d'une majorité écrasante des communications (89,5 %), comme pour l'exercice 2019.
4. L'escroquerie est mentionnée par les intermédiaires financiers comme infraction préalable possible dans 58 % des communications reçues en 2020. Même si des biais statistiques empêchent d'établir une comparaison exacte avec les années précédentes, ce chiffre place clairement l'escroquerie en tête des infractions préalables présumées les plus fréquemment mentionnées par les intermédiaires financiers.
5. Pour la première fois, la surveillance des transactions est mentionnée par les intermédiaires financiers comme l'élément qui contribue le plus à faire émerger les soupçons (cf. ci-après, ch. 4.8).

4.3 Communications de soupçons

Comme la façon de dénombrer les communications des soupçons reçues par le MROS a été adaptée avec l'introduction de goAML, nous nous référons au nombre moyen de relations d'affaires par communication transmise au MROS par les intermédiaires financiers suisses pendant l'exercice 2019 pour permettre une comparaison avec les années précédentes. Ce taux s'élève à 1,8. On peut ainsi estimer que les 5334 communications reçues par le MROS en 2020 correspondent à 9601 relations d'affaires. Selon cette estimation, les communications reçues en 2020 représentent donc une hausse de presque 25 % par rapport à l'exercice précédent, ce qui indique une poursuite de la tendance à l'augmentation du nombre de relations d'affaires signalées, constatée depuis 2015.



4.4 Provenance des communications des intermédiaires financiers par secteur d'activité



- Près de 90 % des communications reçues ont été adressées par des banques.
- Par rapport à l'exercice précédent, la répartition des divers intermédiaires financiers montre une grande stabilité. Comme en 2019, les fiduciaires, les gérants de fortune / conseillers en placement et les maisons de jeu ont adressé 1 % des communications, tandis que les sociétés de transfert de fonds sont passées de 4 % à 3 %.
- La catégorie « autres » regroupe notamment les prestataires de services financiers en crypto-monnaies (*virtual asset service providers* – VASP)[9]. L'augmentation des communications transmises par cette catégorie d'intermédiaires financiers découle partiellement de la façon dont les communications de soupçons sont dénombrées depuis l'introduction de goAML.

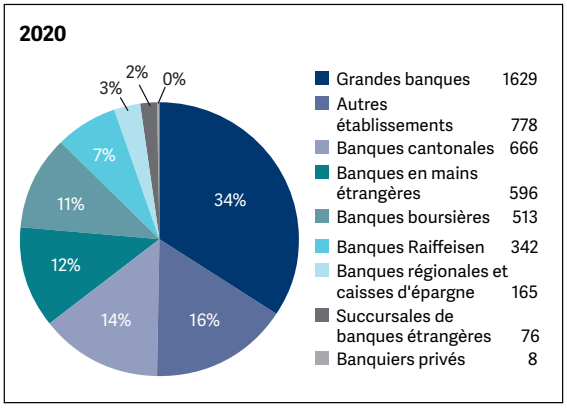
[9] Par VASP, on entend les crypto-bourses, les dépositaires de portefeuilles, les fournisseurs de services financiers en lien avec l'émission, l'offre et la vente de valeurs patrimoniales virtuelles ou d'autres services d'intermédiation financière offerts en relation avec des crypto-monnaies.

Comparaison des années 2011 à 2020[10]

Type d'intermédiaire financier	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 en chiffres absolus	Moyene 2011-2020
Banques	66,5	66,2	79,6	85,3	91,3	86,0	91,0	88,8	89,9	89,5	4773	**83,4**
Prestataires de services de paiement	23,3	22,9	5,2	6,1	2,4	4,4	3,1	4,4	4,0	3,5	185	**7,9**
Autres	0,1	0,3	0,1	0,2	0,2	0,7	0,4	2,3	0,6	2,3	121	**0,7**
Entreprises de cartes de crédit	0,6	1,4	1,0	0,5	0,5	0,7	0,3	1,2	1,3	1,6	83	**0,9**
Gérants de fortune / Conseillers en placement	1,7	3,1	5,2	2,3	1,9	2,2	1,9	1,0	0,9	0,8	45	**2,1**
Fiduciaires	3,8	4,1	4,9	2,8	2,0	1,5	1,1	0,7	0,8	0,6	30	**2,2**
Casinos	0,4	0,4	0,6	0,5	0,1	0,5	0,6	0,5	0,7	0,5	29	**0,5**
Assurances	0,7	0,6	1,3	0,6	0,5	3,1	0,5	0,6	0,3	0,4	20	**0,9**
Opérations de crédit, de leasing, d'affacturage et de financement à forfait	0,3	0,1	0,3	0,2	0,3	0,3	0,3	0,3	0,3	0,4	19	**0,3**
Courtiers en matières premières et métaux précieux	0,1	0,2	0,7	0,2	0,3	0,1	0,2		0,3	0,2	12	**0,2**
Avocats et notaires	1,9	0,8	0,6	0,6	0,3	0,2	0,1	0,1	0,1	0,1	6	**0,5**
Trustees										0,1	4	**0,0**
Bureaux de change	0,2									0,1	3	**0,0**
Négociants en valeurs mobilières	0,0	0,1	0,1	0,6	0,1	0,1	0,3	0,1	0,3	0,0	2	**0,2**
OAR	0,1			0,1					0,1	0,0	2	**0,0**
Négoce de devises	0,4		0,4			0,1			0,3	0,0	0	**0,1**
Autorités				0,1							0	**0,0**
Distributeurs de fonds de placement							0,1				0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**5334**	**100,0**

4.5 Types de banques

Le graphique ci-contre indique le nombre de communications adressées selon le type de banque.



[10] Les chiffres absolus pour les années 2011-2019 sont publiés dans les rapport annuels du MROS des années correspondantes. Par souci d'exhaustivité, il est à noter que les négociants n'apparaissent pas dans cette statistique, puisque le MROS n'a reçu qu'une communication d'un négociant en 2017 et une en 2019, ce qui correspond à moins de 0,1 % du total des communications de soupçons reçues durant ces années.

Comparaison des années 2011 à 2020[11]

Type de banque[12]	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 en chiffres absolus	Moyenne 2011-2020
Banques cantonales	6,9	7,6	6,4	5,0	5,8	7,6	5,2	5,5	5,3	14,0	666	**6,9**
Grandes banques	28,7	29,3	28,9	31,7	35,3	31,1	26,3	26,7	28,2	34,1	1629	**30,0**
Banques régionales et caisses d'épargne	1,4	1,8	0,5	0,9	0,5	1,2	0,6	1,1	1,3	3,5	165	**1,3**
Banques Raiffeisen	5,6	6,1	7,0	9,0	5,8	6,2	3,9	3,2	3,1	7,2	342	**5,7**
Banques boursières	14,4	12,1	10,2	10,6	14,0	12,4	12,7	20,8	25,1	10,7	513	**14,3**
Autres banques	2,5	4,0	20,5	14,3	9,9	12,9	9,6	9,5	8,6	16,3	778	**10,8**
Banquiers privés	2,4	5,7	4,6	2,6	1,8	2,3	1,7	1,9	1,3	0,2	8	**2,5**
Banques en mains étrangères	36,0	33,1	21,4	25,6	26,6	26,3	39,8	31,0	26,9	12,5	596	**27,9**
Succursales de banques étrangères	1,9	0,2	0,4	0,2	0,3	0,1	0,1	0,3	0,2	1,6	76	**0,5**
Établissements à statut particulier	0,1	0,0	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	**0,0**
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**4773**	**100,0**

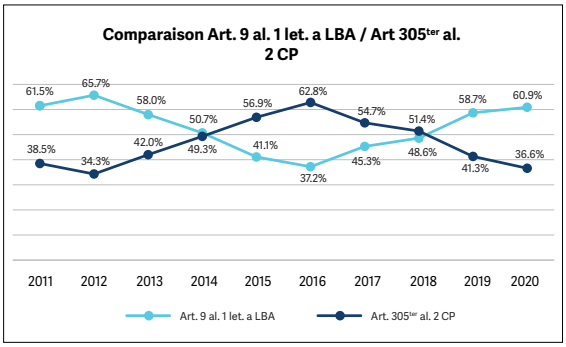
- Le tableau ci-dessus suggère d'importantes variations par rapport à 2019 : le taux de communications émanant des banquiers privés, des banques boursières et des banques en mains étrangères a chuté (respectivement de 1 % à 0 %, de 25 % à 11 % et de 27 % à 12 %), tandis que le pourcentage des communications en provenance des grandes banques, des banques cantonales, des banques Raiffeisen et des autres types d'établissement a augmenté (respectivement de 28 % à 34 %, de 5 % à 14 %, de 3 % à 7 % et de 8 % à 16 %).
- Ces variations s'expliquent en partie du fait que la façon de compter les communications de soupçons a changé (cf. ci-dessus, ch. 4 et 4.3). Le poids des intermédiaires financiers qui ont tendance à effectuer des communications de soupçons portant sur plusieurs relations d'affaires n'est désormais plus aussi grand, puisque ce sont les communications de soupçons – et non les relations d'affaires – qui sont considérées dans la statistique.
- L'augmentation des communications de la part des banques cantonales (de 5,3 % en 2019 à 14,0 % en 2020), s'explique en partie par les nombreuses communications effectuées en lien avec des crédits COVID.

[11] Les chiffres absolus pour les années 2011-2019 sont publiés dans les rapport annuels du MROS des années correspondantes.

[12] Les types de banques et l'ordre indiqué correspond à ceux utilisés par la Banque nationale suisse. Cf. la publication *Les banques en Suisse 2019*, page 9

4.6 Bases légales des communications

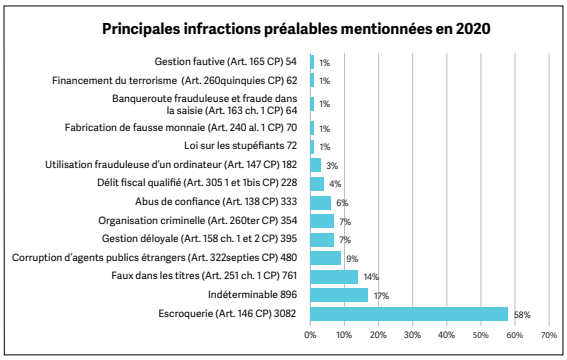
Parmi les 5334 communications reçues au cours de la période sous revue, 3248 relevaient de l'obligation de communiquer au sens de l'art. 9, al. 1, let. a, LBA (60,9 %) et 1952 (36,6 %) du droit de communiquer au sens de l'art. 305ter, al. 2, Code pénal suisse du 21 décembre 1937 (CP[13]). Par ailleurs, 129 communications ont également été adressées au titre de l'art. 9, al. 1, let. b, LBA (2,4 %) et 2 au titre de l'art. 27, al. 4, LBA.



Ainsi, la hausse relative du taux de communication selon l'art. 9, al. 1, let. a, LBA, constatée depuis 2016, se poursuit. Comme la grande majorité des communications reçues par le MROS sont rédigées par les banques, cette tendance illustre surtout le comportement du secteur bancaire. Néanmoins, parmi les banques suisses auteures des communications, le recours à l'art. 9, al. 1, let. a, LBA ou à l'art. 305ter, al. 2, CP est très différencié en fonction du type d'établissement, ainsi que le montre le tableau suivant.

4.7 Infractions préalables

Le graphique ci-dessous indique le taux de mention d'une infraction préalable présumée parmi les communications reçues en 2020. Contrairement à ce qui prévalait jusqu'en 2019, l'intermédiaire financier auteur d'une communication de soupçons peut désormais indiquer, pour chaque communication, plusieurs infractions préalables potentielles. En conséquence, s'il est possible de déterminer le taux de mention d'une infraction préalable parmi les communications reçues, la somme de ces taux dépasse 100 %, de sorte que leur comparaison avec les taux des années précédentes est biaisée et ne peut être qu'indicative.



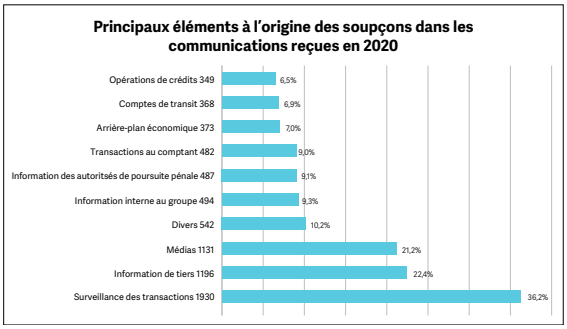
Type de banque	Art. 9 al. 1 let. a LBA	en %	Art. 305ter al. 2 CP	en %	Autre	en %	Total général	en %
Banques cantonales	554	83,1	106	15,9	6	0,9	666	100,0
Grandes banques	790	48,5	829	50,8	10	0,6	1629	100,0
Banques régionales et caisses de épargne	97	58,7	60	36,3	8	4,8	165	100,0
Banques Raiffeisen	305	89,1	28	8,1	9	2,6	342	100,0
Banques boursières	230	44,8	250	48,7	33	6,4	513	100,0
Autres établissements	663	85,2	101	12,9	14	1,8	778	100,0
Banquiers privés	3	37,5	5	62,5	0	0,0	8	100,0
Banques en mains étrangères	301	50,5	269	45,1	26	4,3	596	100,0
Succursales de banques étrangères	12	15,7	64	84,2	0	0,0	76	100,0
Total	**2955**	**61,9**	**1712**	**35,8**	**106**	**2,2**	**4773**	**100,0**

13 RS **311.0**

– Les importantes variations constatées entre 2020 et les années précédentes s'expliquent en partie par la possibilité désormais offerte aux intermédiaires financiers de mentionner plusieurs infractions préalables possibles, parmi une liste générale qui a été mise à jour et augmentée.
– Néanmoins, l'année sous revue a connu une explosion du nombre de soupçons d'escroquerie, qui était associée à 25 % des communications reçues en 2019 et à 20 % en 2018, mais qui est mentionnée dans 58 % des communications reçues en 2020. Cette évolution résulte en partie du nombre important de communications reçues en relation avec l'octroi de crédits COVID (cf. ch. 5.1).
– 2020 a également connu une chute drastique des communications pour lesquelles l'infraction préalable soupçonnée était la corruption. La corruption d'agents publics étrangers est mentionnée dans 480 communications, soit 9 % ; la corruption active d'agents publics suisses dans 21 communications, soit 0,39 % et la corruption passive d'agents publics suisses dans 17 cas, soit 0,32 %. Ces trois catégories, qui n'étaient pas distinguées dans les rapports précédents, représentaient 24 % des communications reçues en 2019 et 27 % de celles reçues en 2018.
Il est difficile d'interpréter de telles variations d'une année à l'autre. La baisse des soupçons de blanchiment d'argent associés à des faits de corruption s'explique en partie par le fait que certains affaires complexes internationales qui ont influencé dans les dernières années la place financière suisse et qui ont suscitées de nombreuses communications au MROS n'en suscitent plus guère.

4.8 Éléments à l'origine des soupçons

Le graphique ci-contre indique le taux de mention des éléments à l'origine des soupçons parmi les communications reçues en 2020. Comme pour les infractions préalables et contrairement à ce qui prévalait par le passé, le nouveau système d'information goAML permet aux intermédiaires financiers de signaler plusieurs éléments qui les ont portés à concevoir des soupçons. En conséquence, il est possible de calculer dans quelle proportion des communications reçues un élément en particulier a été déterminant, mais il n'est plus possible d'effectuer une comparaison précise de ces chiffres avec ceux des années antérieures.



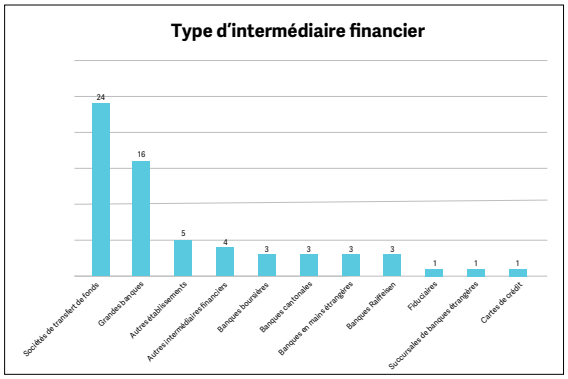
– La comparaison avec les années précédentes, où seul un élément à l'origine des soupçons pouvait être enregistré, n'est pas pertinente.
– Néanmoins, pour la première fois pendant l'année sous revue, la surveillance des transactions est l'élément à l'origine des soupçons le plus souvent mentionné (36,2 % en 2020, contre 31 % en 2019 et 25 % en 2018). Ceci confirme la sensibilisation accrue des intermédiaires financiers dans les clarifications et les analyses d'ordre transactionnel au sens de l'art. 6 al. 2 LBA.
– Les informations des médias, origine principale des soupçons des intermédiaires financiers au cours des années précédentes, ont été nettement moins déterminants en 2020 (21,2 % des cas, contre 35 % en 2019 et 38 % en 2018).

4.9 Financement du terrorisme

Pendant l'année sous revue, 64 communications ont été adressées au MROS pour signaler un soupçon de financement du terrorisme et/ou d'infraction à la loi fédérale interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées[14], soit 1,2 % du total

[14] RS **122**

des communications reçues. Dans la mesure où l'on estime qu'il y a environ 1,8 relation d'affaires par communication, ces 64 communications comprennent environ 115 relations d'affaires, soit un nombre presque égal à celui de 2019 (114). Ces 64 communications sont également associées à d'autres infractions préalables, soit l'appartenance à une organisation criminelle (19 cas), l'escroquerie (7 cas), la corruption d'agents publics étrangers (3 cas), tandis que d'autres infractions préalables supposées sont mentionnées dans dix cas.
L'élément à l'origine des soupçons le plus souvent cité pour ces communications par les intermédiaires financiers – notamment par les sociétés de transfert de fonds – est la surveillance des transactions (33 cas), suivi des articles de presse (20 cas), des transactions au comptant (15 cas), des informations de tiers (13 cas), des liens avec des pays sensibles (8 cas), tandis que d'autres éléments sont cités dans 12 cas.
La majorité des communications (34) ont été adressées par des banques, tandis que des sociétés de transfert de fonds en ont établi 24. Seules 6 de ces communications ont été effectuées par d'autres types d'intermédiaires financiers.



Parmi ces 64 communications, 47 n'ont pas fait l'objet dénonciation par le MROS ; deux étaient encore en cours d'analyse au MROS à la fin de l'année sous revue. Les informations tirées des 15 communications restantes ont alimenté 14 dénonciations aux autorités de poursuite pénale compétentes. Dans trois cas, des procédures pénales sont formellement ouvertes, mais l'une d'entre elles est ouverte pour des faits de trafic d'êtres humains et non pour des violations à la loi fédérale interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées.

4.10 Criminalité organisée

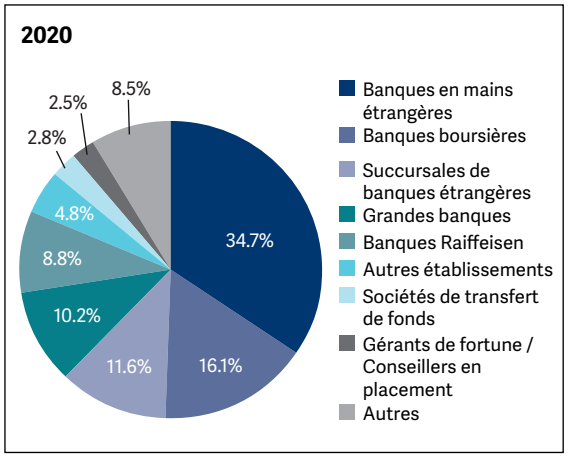
En 2020, le MROS a reçu 354 communications mentionnant des soupçons de liens avec une organisation criminelle, soit 6,6 % du total des communications reçues. Un tel pourcentage indique une augmentation par rapport à 2019, où les communications portant sur de tels soupçons ne constituaient que 2,4 % du total des relations d'affaires annoncées. Il faut toutefois garder à l'esprit les biais statistiques évoqués plus haut qui rendent difficile la comparaison avec les chiffres des années précédentes.
Pendant l'année sous revue, les communications faisant état de soupçons de liens avec une organisation criminelle mentionnaient également d'autres infractions préalables potentielles : la corruption d'agents publics étrangers (111 cas), l'escroquerie (72 cas), la fabrication de fausse monnaie (67 cas), le faux dans les titres (26 cas) et le financement du terrorisme (23 cas).

Principales autres infractions préalables mentionnées dans les communications de soupçons en lien avec le soupçon d'appartenance à une organisation criminelle	Nombre de mentions	en %
Corruption d'agents publics étrangers	111	31,4
Escroquerie	72	20,3
Fabrication de fausse monnaie	67	18,9
Faux dans les titres	26	7,3
Financement du terrorisme	23	6,5
Loi sur les stupéfiants	20	5,6
Abus de confiance	12	3,4
Gestion déloyale	9	2,5
Extorsion et chantage	5	1,4
Loi sur les armes	4	1,1
Vol	2	0,6
Gestion déloyale des intérêts publics	2	0,6
Corruption d'agents publics suisses, corruption active	1	0,3

Pendant l'exercice sous revue, les éléments suivants étaient à l'origine des communications adressées au MROS qui mentionnaient l'appartenance à une organisation criminelle comme infraction présumée :

Eléments à l'origine du soupçon	Nombre de mentions	En %
Médias	168	47,5
Surveillance des transactions	115	32,5
Transactions au comptant	82	23,2
Divers	76	21,5
Informations de tiers	42	11,9
Information interne au groupe	28	7,9
Informations des autorités de poursuite pénale	20	5,6
Ouverture de relations d'affaires	18	5,1
Pays sensibles	16	4,5

Dans leur écrasante majorité (88,7 %), les communications de soupçons présentant des liens avec une organisation criminelle ont été adressées au MROS par des banques, suivies des sociétés de transfert de fonds (2,82 %), des gérants de fortune / conseillers en placement (2,54 %) et des assurances (2,26 %). Parmi les banques, les principaux types d'établissement à l'origine de ces communications sont les suivants :



Parmi ces 354 communications, 256 (soit 73,2 %) n'ont pas fait l'objet d'une dénonciation de la part du MROS aux autorités de poursuite pénale et 24 sont encore en cours d'analyse. Sur la base de 74 communications, le MROS a effectué 46 dénonciations aux autorités de poursuite pénale compétentes. Huit d'entre elles ont fait l'objet d'ordonnances de non-entrée en matière, tandis que les 38 autres sont en cours d'examen par les autorités de poursuite pénale compétentes.

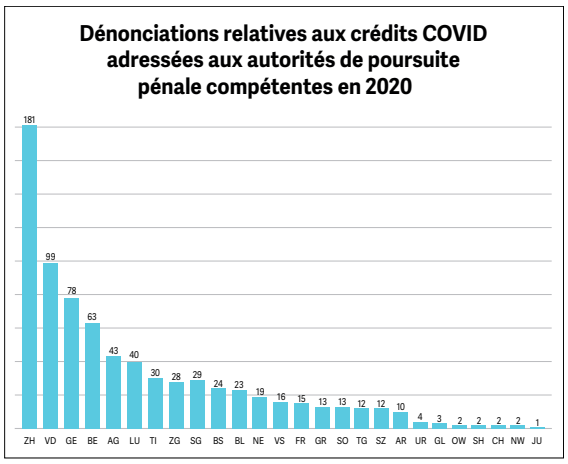
4.11 Pandémie COVID

La pandémie due au COVID qui a marqué l'année 2020 a offert aux criminels plusieurs opportunités d'enrichissement illégal, augmentant ainsi les risques de blanchiment d'argent. Parmi les différentes typologies de blanchiment d'argent supposé qui ressortent des communications adressées au MROS pendant l'année sous revue (cf. ci-après, ch. 5.1), le détournement ou l'utilisation frauduleuse des crédits accordés par les institutions financières suisses sous le cautionnement de la Confédération s'est reflété dans les statistiques du MROS. Entre l'introduction de ces crédits par l'ordonnance du Conseil fédéral du 25 mars 2020[15] et la fin de l'année 2020, le MROS a reçu 1046 communications de soupçons relevant de cette typologie. Elles concernaient 1054 crédits COVID, accordés par 43 banques différentes, pour une somme totale de 146 853 347 CHF.[16] En 2020, le MROS a transmis 764 dénonciations aux autorités de poursuite pénale en relation avec 914 communications. 27 communications effectuées en relation avec des crédits COVID étaient encore en cours d'analyse à la fin de l'exercice sous revue.

Les autorités de poursuite pénale auxquelles ces dénonciations ont été adressées et le nombre des dénonciations sont indiquées dans le graphique ci-dessous. Suite aux transmissions du MROS, les autorités de poursuite pénale ont ouvert plusieurs centaines d'instructions pénales, ce qui confirme le rôle central que le MROS a joué dans ce développement inattendu (cf. ci-dessous, ch. 5.1).

[15] RS **951.261.** Celle-ci a été remplacée, en date du 19 décembre 2020, par la loi fédérale du 18 décembre 2020 sur les crédits garantis par un cautionnement solidaire à la suite du coronavirus (Loi sur les cautionnements solidaires liés au COVID-19, LCaS-COVID-19 ; RS **951.26**).

[16] Cf. les statistiques publiées à ce sujet sur la page Internet du MROS : *Crédits COVID-19*.



Légende

AG	Argovie	NW	Nidwald
AI	Appenzell Rhodes intérieures	OW	Obwald
AR	Appenzell Rhodes extérieures	SG	Saint-Gall
BE	Berne	SH	Schaffhouse
BL	Bâle-Campagne	SO	Soleure
BS	Bâle-Ville	SZ	Schwytz
CH	Ministère public de la Confédération	TG	Thurgovie
FR	Fribourg	TI	Tessin
GE	Genève	UR	Uri
GL	Glaris	VD	Vaud
GR	Grisons	VS	Valais
JU	Jura	ZG	Zoug
LU	Lucerne	ZH	Zurich
NE	Neuchâtel		

4.12 Dénonciations aux autorités de poursuite pénale

En 2020, le MROS a transmis 1939 dénonciations aux autorités de poursuite pénale. Avec l'adaptation de l'OBCBA entrée en vigueur le 1er janvier 2020, les communications de soupçons ne sont plus transmises aux autorités de poursuite pénale. Afin de garantir la protection des sources – aucune indication relative à l'auteur de la communication ou à la personne ayant communiqué des informations n'est transmise aux autorités de poursuite pénale (cf. art. 8, al. 1, OBCBA).[17] Les informations pertinentes et l'évaluation que le MROS en fait sont adressées aux Ministères publics sous forme de rapports électroniques. Les dénonciations destinées aux autorités de poursuite pénale peuvent contenir des informations provenant de différentes sources ou de différentes communications (cf. art. 1, al. 2, let. a-e, OBCBA). Même si en pratique, il arrive souvent qu'une transmission contienne en premier lieu les informations d'une communication, ce cas de figure classique n'est plus la règle. C'est la nature agrégée des informations enregistrées par le MROS qui détermine leur sort. Comme annoncé dans notre rapport d'activité 2019[18] déjà, la notion de « taux de transmission » des communications de soupçons n'est par conséquent plus pertinente. En effet, comme les dénonciations effectuées peuvent contenir des informations provenant de plusieurs sources différentes et de plusieurs communications, parfois reçues à des années différentes, elles ne peuvent plus être rapportées au nombre de communications reçues pendant une année particulière. Les dénonciations effectuées en 2020 comprenaient des informations provenant de :

- 2156 communications reçues en 2020
- 179 relations d'affaires signalées en 2019
- 52 relations d'affaires signalées en 2018
- 12 relations d'affaires signalées en 2017
- 3 relations d'affaires signalées en 2016
- 1 relation d'affaires signalées en 2014
- 4 relations d'affaires signalées en 2011.

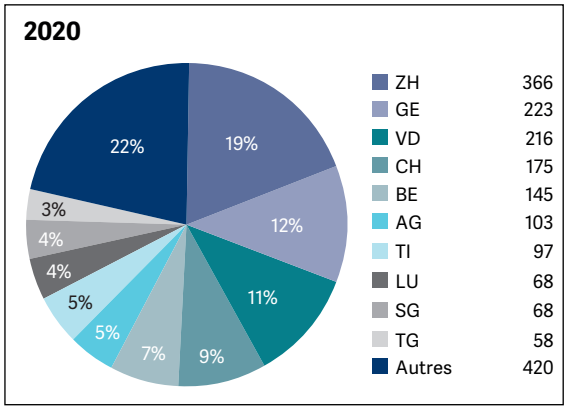
Les chiffres relatifs aux communications reçues après le 22 novembre 2019[19], soit 2235 cas, concernent des communications pouvant contenir plusieurs relations d'affaires. Les chiffres elatifs à la période antérieure correspondent à une relation d'affaires.

17 Cf. les *commentaires sur la révision partielle de l'OBCBA* du 24 novembre 2019, p. 9-10 ainsi que p. 16.

18 Cf. *rapport annuel 2019 du MROS,* p. 9.

19 À partir de cette date, le MROS a enregistré les communications reçues dans le système d'informations goAML. 76 des 179 communications reçues en 2019 qui ont alimenté des dénonciations du MROS aux autorités de poursuite pénale en 2020 étaient dans ce cas. Ces 76 communications portaient sur 153 relations d'affaires, de sorte que le nombre total de relations d'affaires signalées en 2019 au MROS et qui ont alimenté des dénonciations adressées aux autorités de poursuite pénale en 2020 s'élève à 256.

Autorités de poursuite pénale concernées
Le graphique ci-dessous indique à quelles autorités de poursuite pénale les 1939 dénonciations effectuées en 2020 par le MROS ont été transmises.



Pour des raisons statistiques et à cause de la différente façon de dénombrer les communications de soupçons, la comparaison avec les années précédentes n'est guère pertinente. Depuis l'introduction du système goAML, les dénonciations peuvent comprendre plusieurs communications portant sur plusieurs relations d'affaires, mais les informations transmises peuvent également être tirées d'autres sources que les communications.
Pour la première fois, le Ministère public de la Confédération (MPC) n'a pas été l'autorité de poursuite pénale la plus sollicitée par le MROS. Il n'a reçu que 9 % des dénonciations effectuées en 2020, contre 40 % en 2019 et 49 % en 2018. Cette baisse doit toutefois être nuancée : les dénonciations adressées au MPC portent le plus souvent sur des faits de blanchiment associé à

Comparaison des années 2011 à 2020

Autorité	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 en chiffres absolus	Moyene 2011-2020
ZH	19,7	14,4	18,4	12,4	13,5	12,0	10,2	12,8	14,3	18,9	366	14,7
GE	12,6	15,1	15,0	12,7	8,4	14,9	12,8	14,1	15,0	11,5	223	13,2
VD	4,7	2,1	2,4	2,5	2,6	3,1	1,8	4,3	5,5	11,1	216	4,0
CH	31,9	35,8	34,2	44,7	53,4	38,1	52,6	48,4	39,9	9,0	175	38,8
BE	3,2	3,8	1,6	4,6	1,8	3,0	1,6	1,8	3,3	7,5	145	3,2
AG	3,3	2,0	1,3	1,8	1,5	2,6	1,2	1,6	1,5	5,3	103	2,2
TI	8,5	13,6	12,5	7,3	6,5	6,0	6,0	3,3	3,3	5,0	97	7,2
SG	4,5	2,2	1,7	3,0	2,0	2,2	2,4	1,3	1,2	3,5	68	2,4
LU	0,6	1,1	1,5	1,8	1,0	1,4	1,4	0,8	1,8	3,5	68	1,5
TG	0,6	1,1	0,7	1,1	0,8	1,5	0,7	0,8	1,3	3,0	58	1,2
FR	0,7	1,2	0,5	0,2	0,6	0,6	1,4	1,6	1,5	2,7	53	1,1
VS	0,5	0,4	1,1	1,0	0,5	1,0	1,2	1,4	0,8	2,7	53	1,1
BS	3,4	2,7	2,2	1,2	1,3	3,3	2,0	0,9	0,9	2,6	50	2,0
ZG	1,3	0,6	1,2	1,3	1,5	1,2	0,6	1,9	1,9	2,5	49	1,4
NE	0,7	0,6	0,7	0,9	1,1	0,9	1,0	1,2	1,4	2,3	44	1,1
BL	0,5	1,3	0,8	0,5	1,5	1,5	1,2	0,8	2,9	2,1	41	1,3
SO	0,9	0,1	1,1	0,7	0,4	4,2	0,4	1,1	1,2	1,9	37	1,2
GR	0,5	0,5	0,9	1,0	0,6	0,3	0,5	0,3	0,4	1,5	29	0,7
SZ	0,6	0,6	0,6	0,2	0,5	0,8	0,5	0,3	0,4	1,0	20	0,6
AR	0,1	0,1	0,2	0,2	0,1	0,3	0,2	0,2	0,3	0,6	12	0,2
SH	0,5	0,4	0,6	0,3	0,1	0,5	0,3	0,1	0,3	0,5	10	0,4
UR	0,0	0,0	0,0	0,1	0,0	0,2	0,0	0,0	0,0	0,3	6	0,1
NW	0,3	0,0	0,4	0,1	0,1	0,0	0,0	0,7	0,2	0,3	5	0,2
JU	0,1	0,1	0,2	0,6	0,0	0,3	0,1	0,1	0,1	0,3	5	0,2
GL	0,0	0,0	0,1	0,0	0,0	0,1	0,1	0,2	0,0	0,2	3	0,1
OW	0,1	0,2	0,0	0,0	0,1	0,0	0,0	0,0	0,3	0,2	3	0,1
AI	0,1	0,1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0	0,0
Total	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**100,0**	**0**	**100,0**

des infractions préalables commises à l'étranger. Elles présentent donc un degré de complexité supérieur et les informations dont elles sont composées sont plus fréquemment tirées de différentes communications, portant sur plusieurs relations d'affaires. Au contraire, dans les transmissions aux autorités de poursuite pénale cantonales, la source d'une dénonciation est généralement composée d'une seule communication de soupçons.
Le nombre de dénonciations adressées aux autorités de poursuite pénale du canton de Zurich excède en 2020 largement celles à destination du canton de Genève (19 % contre 12 %), alors que jusqu'à présent les deux cantons recevaient un nombre à peu près équivalent de dénonciations de la part du MROS, voire un nombre légèrement supérieur à Genève.
Pour la première fois également, plus de dénonciations ont été effectuées aux autorités de poursuites pénales des cantons de Vaud, de Berne et d'Argovie qu'à celles du Tessin. Ensemble, les 17 autres cantons ont reçu davantage de dénonciations du MROS que Zurich (420 contre 366). Cette situation tranche avec ce qui prévalait jusqu'en 2019, où les 17 ou 18 cantons les moins sollicités par le MROS ne totalisaient que rarement plus de 15 % des transmissions.
Au-delà des changements introduits par le système d'information goAML qui rendent les comparaisons avec les années précédentes difficiles, les variations constatées sont également dues au traitement des nombreuses communications qui ont été adressées au MROS à propos de soupçons liés à des crédits COVID. Cela explique partiellement le taux moindre de dénonciations au MPC, qui n'est généralement pas compétent pour traiter de ce genre d'affaires. Ceci explique également le nombre plus important de dénonciations adressées aux cantons de Vaud, de Berne et d'Argovie qu'au Tessin.

4.13 Communications des années 2016-2019 encore en cours d'analyse

À la fin de l'exercice 2019, un nombre total de 6095 relations d'affaires annoncées au MROS durant les années 2016 à 2019 étaient toujours en cours d'analyse (10 de 2016, 737 de 2017, 1717 de 2018 et 3631 de 2019). Pendant l'exercice sous revue, le MROS a développé un effort particulier pour traiter ces relations d'affaires signalées. La plupart de ces relations d'affaires n'ont pas abouti à des transmissions (94,5 %), tandis que 4,9 % d'entre elles ont alimenté des dénonciations effectuées aux autorités de poursuite pénale compétentes. À la fin 2020, seules 37 d'entre elles (0,6 %) sont encore en cours d'analyse. Le tableau ci-dessous en donne le détail, en fonction de l'année de réception de ces relations d'affaires.

Année de la réception	2016	2017	2018	2019	Total
Décision de non-transmission	10	730	1680	3342	5762
Dénonciation		6	34	256	296
En cours d'analyse		1	3	33	37
Total	**10**	**737**	**1717**	**3631**	**6095**

4.14 Échanges avec les homologues étrangers (CRF)

Le MROS et ses homologues étrangers, c'est-à-dire les autres CRF, peuvent échanger par la voie de l'assistance administrative internationale des informations concernant la lutte contre le financement du terrorisme, le blanchiment d'argent et les infractions préalables qui s'y rapportent ou contre la criminalité organisée. Lorsque le MROS reçoit des communications de soupçons impliquant des personnes physiques ou morales étrangères, il a la possibilité de demander des informations au sujet de ces personnes ou de ces sociétés à ses homologues des pays concernés. Les renseignements obtenus sont importants pour l'analyse du MROS, car la plupart des communications de soupçons parvenant au MROS présentent des éléments d'extranéité.
En 2020, le Bureau de communication a reçu 795 demandes de 95 pays, soit une légère diminution par rapport à l'exercice précédent (2019 : 844 demandes de 103 pays). Le MROS a traité 684 de ces demandes, soit 86 %. La durée moyenne de traitement de ces demandes était de 41 jours ouvrés. En outre, le MROS a également répondu en 2020 à 173 demandes d'informations qui lui avaient été adressées en 2019.
Le nombre de personnes physiques et morales faisant l'objet des demandes d'informations

étrangères traitées en 2020 s'élève à 5212 au total (2733 personnes morales et 2479 personnes physiques). 4169 d'entre elles (2155 personnes morales et 1994 personnes physiques) étaient l'objet des demandes d'informations étrangères reçues et traitées en 2020.
Les informations spontanées sont des informations communiquées par un homologue étranger présentant un lien avec la Suisse qui ne requièrent pas de réponse, ou à l'inverse communiquées par la CRF suisse à des homologues étrangers. Depuis 2015, le nombre d'informations dites spontanées qui sont traitées dans l'année est distingué des demandes d'informations.
Durant l'année sous revue, le MROS a reçu 504 informations spontanées de 47 pays et en a envoyé 365 à 76 CRF étrangères.
En 2020, le MROS a adressé 126 demandes d'information à 46 homologues étrangers différents. Ces demandes portaient sur 364 personnes morales et 303 personnes physiques. En moyenne, les CRF contactées ont répondu aux demandes dans un délai d'environ 30 jours.

4.15 Échanges avec les autorités nationales

Les échanges d'informations auxquels le MROS procède ne s'effectuent pas uniquement avec ses homologues étrangers, mais également avec d'autres autorités suisses comme les autorités de surveillance ou d'autres autorités actives dans la lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme. Le MROS est habilité à échanger des informations avec ces autorités aux conditions de l'art. 29 LBA. Les statistiques de ces échanges n'ont pas été publiées dans les rapports annuels précédents. Ces échanges ont désormais acquis une importance nouvelle, à la fois du point de vue de leur contenu et de la charge qu'ils représentent pour le MROS.
En 2020, le MROS a été sollicité à 392 reprises par 26 autorités helvétiques qui lui demandaient des informations à propos de personnes et sociétés particulières, dans le cadre d'enquêtes sur des faits de blanchiment d'argent, de criminalité organisée ou de financement du terrorisme. Dans approximativement 80 % des cas, ces demandes émanaient de polices cantonales et de la Police judiciaire fédérale. Ces 392 demandes d'informations correspondent à une augmentation de plus de 200 % par rapports aux exercices précédents : en 2018 comme en 2019, le nombre de demandes d'informations d'autres autorités suisses au MROS s'élevait à 117.
Le rôle du MROS vis-à-vis des autres autorités suisses impliquées dans la lutte contre le blanchiment d'argent, ses infractions préalables, la lutte contre la criminalité organisée et le financement du terrorisme ne se limite pas à répondre à leurs demandes d'informations. Dans le cadre de ses analyses, le MROS est également habilité à transmettre spontanément les informations dont il dispose à d'autres autorités suisses actives dans la vigilance en matière d'opérations financières et de lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme. En 2020, le Bureau de communication a transmis 69 informations spontanées dans ce contexte. En outre, le MROS peut requérir les informations dont il a besoin pour effectuer ses analyses auprès d'autres autorités fédérales, cantonales et communales. Ces dernières demandes ne sont pas répertoriées dans les chiffres ci-dessus.

5. Typologies destinées à la sensibilisation des intermédiaires financiers

Les typologies suivantes ne font volontairement pas référence à des communications de soupçons représentatives de l'année 2020, mais à des faits qui sont relativement peu signalés, exception faite des cas autour de la pandémie de COVID (cf. ch. 5.1). En 2020, les communications de soupçons en lien avec des organisations criminelles et le financement du terrorisme ne représentaient par exemple que 7,8 % du nombre total de communications transmises au MROS. Ces deux champs d'infraction comptent parmi ceux qui sont au cœur de la stratégie 2020-2023 du DFJP en matière de lutte contre la criminalité. Ces typologies présentent des exemples concrets illustrant comment les produits des infractions présumées sont blanchis. Les cas choisis reflètent aussi les nouvelles tendances et les méthodes utilisées, et permettent d'en tirer des conclusions. Ces typologies sont destinées à sensibiliser les intermédiaires financiers en attirant leur attention sur les types de comptes, d'instruments financiers ou de comportements qui doivent faire l'objet d'une attention particulière de leur part selon les risques constatés par le MROS.

5.1 Cas découlant de la situation créée par la pandémie COVID

Une partie notable de l'augmentation des communications reçues par le MROS en 2020 s'explique par le signalement de soupçons de blanchiment d'argent en lien avec la pandémie de COVID. De tels liens concernent près d'un tiers des communications adressées au MROS en 2020. La situation particulière créée par la pandémie a offert aux criminels plusieurs opportunités d'enrichissement illégal, augmentant ainsi les risques de blanchiment d'argent. Les risques identifiés à l'échelle internationale en relation avec la lutte contre le blanchiment d'argent, les organisations criminelles et le financement du terrorisme sont de nature très diverse.[20] Ils couvrent un spectre allant du détournement des sommes mises à disposition par des organisations étatiques ou supranationales pour la lutte contre la pandémie aux risques provoqués par l'augmentation de la cybercriminalité, attisée par le recours généralisé au travail à distance, en passant par des escroqueries commises dans le cadre de la commercialisation de matériel sanitaire ou par les risques accrus d'infiltration de valeurs patrimoniales illicites dans les secteurs économiques en difficulté. A titre préventif, le MROS a rendu les intermédiaires financiers suisses attentif aux risques liés à la pandémie, respectivement aux crédits COVID par le biais de goAML les 2 et 29 avril 2020.
Parmi les communications de soupçons reçues par le MROS, trois risques spécifiques de blanchiment liés à l'épidémie émergent. Le premier relève du détournement ou de l'utilisation indue des prêts accordés aux entreprises avec la garantie des autorités publiques helvétiques. Le 25 mars 2020, le Conseil fédéral a promulgué une ordonnance sur les cautionnements solidaires liés au COVID-19[21], qui a permis aux entreprises indivi-

[20] Dès le printemps 2020, plusieurs organismes nationaux et internationaux ont publié des analyses et des mises en garde à ce sujet. Voir par exemple l'analyse (www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html) publiée à ce titre par le GAFI en mai 2020, et actualisée en décembre.

[21] Cf. note 15

duelles, sociétés de personnes ou personnes morales ayant leur siège en Suisse, d'obtenir auprès des institutions de crédit helvétiques des prêts garantis par la Confédération à des conditions facilitées. Cette ordonnance a été remplacée, en date du 19 décembre 2020, par la loi fédérale du 18 décembre 2020 sur les cautionnements solidaires liés au COVID-19 (LCaS-COVID-19).[22]
Le risque que ces crédits soient détournés est manifeste. Durant l'année 2020, le MROS a reçu plus de 1000 communications portant sur plus de 1100 crédits[23] de la part d'intermédiaires financiers alertés par le retrait en liquide ou le transfert des fonds accordés à ce titre vers des comptes personnels, par des chiffres d'affaires visiblement grossis ou par l'utilisation des crédits en contravention des conditions énoncées par l'ordonnance du Conseil fédéral. Plus de 800 dénonciations ont été adressées par le MROS à ce titre aux autorités de poursuite pénale compétentes, notamment pour des soupçons d'escroquerie et/ou de faux dans les titres et gestion déloyale. Suite aux dénonciations du MROS, les autorités de poursuite pénale ont ouvert plusieurs centaines d'instructions pénales.
Une autre typologie de criminalité économique favorisée par la pandémie concerne les escroqueries sur Internet de type *phishing* ou *social engineering*. Les infractions préalables de cette espèce ne sont pas intrinsèquement liées au COVID, mais elles sont devenues plus fréquentes en raison des mesures de confinement imposées dans de nombreux pays. Celles-ci ont poussé vers Internet une population qui s'en tient habituellement à l'écart, plus vulnérable aux arnaques qui y prolifèrent. Sensible dans la plupart des pays, l'augmentation des cas de ce type s'est également traduite par une légère hausse des communications adressées au MROS pour de tels faits.
Alors que les sommes impliquées dans les cas de cette dernière typologie sont généralement modestes, ce n'est pas le cas de ceux qui relèvent d'infractions commises dans le cadre du commerce de matériel sanitaire, qui portent le plus souvent sur plusieurs millions de francs. Les commandes massives de masques, de liquide hydro-alcoolique ou d'autres produits sanitaires par les autorités étatiques, et parfois par des sociétés privées, ont été passées dans une situation d'urgence qui a favorisé les abus et parfois les fraudes. Le matériel vendu peut être inopérant ou de mauvaise qualité, ou son prix gonflé, ou encore ne jamais être délivré. En outre, l'angoisse suscitée par la maladie a fréquemment conduit la population à s'approvisionner elle-même en matériel de ce type, souvent sur Internet, et à prêter attention à de la publicité mensongère vantant de façon frauduleuse les mérites de médicaments prétendument efficaces contre la contamination. Les cas de ce type concernent quelques dizaines de signalements. Ils portent sur des soupçons d'escroqueries commises à l'étranger plus fréquemment qu'en Suisse même. Les principaux éléments à l'origine des soupçons sont l'authenticité douteuse des contrats présentés pour justifier les transactions, le brusque changement d'activités de sociétés ne témoignant d'aucune activité dans le domaine du commerce de matériel sanitaire, la multiplication suspecte des intermédiaires entre le fournisseur et l'acquéreur, mais aussi des articles de presse visant des sociétés pratiquant des prix trop élevés pour le matériel fourni ou des demandes de retour de fonds de la part des banques des acquéreurs lésés.

Blanchiment d'argent présumé dans le contexte de la commercialisation de matériel sanitaire
Un intermédiaire financier relève, sur une relation d'affaires ouverte au nom d'une société de domicile d'une juridiction du Pacifique destinée à la gestion patrimoniale, trois transferts en provenance d'un pays tiers pour un total de plusieurs dizaines de millions de francs. La société de domicile en question appartient à un citoyen européen, actif dans le secteur extractif et domicilié dans un pays du Golfe. Aux dires du client, ces fonds correspondraient à la vente de 10 millions de masques médicaux répondant aux besoins d'un État. Les fonds proviennent d'un compte

[22] Cf. note 15

[23] Cf. les statistiques publiées à ce sujet sur la page Internet du MROS: *Crédits COVID-19.*

ouvert au nom d'un organisme public. Le client agirait comme intermédiaire entre celui-ci et des fournisseurs étrangers. Une partie des sommes entrées sur le compte est virée peu après sur diverses relations bancaires ouvertes dans le pays de ces fournisseurs. L'intermédiaire financier relève plusieurs incohérences entre les informations obtenues auprès du client et la situation dans l'État agissant comme acheteur, doute de la vraisemblance des transactions commerciales et soupçonne une escroquerie ou une gestion déloyale des intérêts publics. Les clarifications entreprises par le MROS ont montré qu'en dépit de son caractère inusuel, la transaction en question avait été dûment autorisée et que les masques commandés avaient bel et bien été livrés. La CRF du pays dans lequel les masques ont été commandés a été informée du caractère inusuel de cette transaction.

Au-delà des trois types de risque liés à la pandémie COVID dont témoignent les communications reçues par le MROS, d'autres risques sont avérés sans que cette source d'information n'en reflète l'intensité. C'est en particulier le cas du blanchiment d'argent commis par des organisations criminelles, qui profitent de la crise sanitaire actuelle et de ses conséquences économiques pour étendre leur emprise, par exemple, en acquérant des sociétés helvétiques endettées ou des biens immobiliers auprès de personnes morales ou physiques éprouvées financièrement. Alors que ce risque accru d'infiltration des organisations criminelles dans l'économie a été signalé par plusieurs instances internationales et qu'il a été documenté par de nombreuses enquêtes de journalistes, le MROS n'a reçu que deux communications qui s'y rapportent. Notons cependant que dans certains cas, les fraudes au crédit signalées semblent avoir été commises par des individus en rapport entre eux ou du moins selon un modus operandi analogue. À ce stade, le MROS n'a néanmoins pas d'indice de l'implication d'organisations criminelles connues dans des schémas de ce type.

Un crédit COVID pour la société d'une personne appartenant à une organisation criminelle ?
Un intermédiaire financier relève le remboursement d'un prêt privé – ce qui est interdit par l'art. 2, al. 2, let. b, LCas-COVID-19 – sur une relation d'affaires ouverte avec une société active dans le secteur de l'entretien et la réparation de véhicules, ayant sollicité un crédit COVID. En effectuant des clarifications supplémentaires, il découvre des articles de presse évoquant l'arrestation du détenteur de la société dans un pays tiers pour appartenance à une organisation criminelle. La relation en question montre essentiellement des apports en numéraire et des transactions avec des comptes de tiers, ouverts dans le pays en question. Les sommes impliquées se montent à plusieurs dizaines de milliers de francs.

5.2 Organisations criminelles

Les faits signalés au MROS en lien avec des organisations criminelles indiquent que des articles de presse ou des éléments issus de banques de données privées sont le plus souvent à l'origine des soupçons des instituts déclarants.
Les comptes de membres d'organisations criminelles ne font souvent apparaître aucun schéma de transaction particulier, si bien qu'ils ne sont pas qualifiés de « suspects » et ne sont pas signalés.
La difficulté des intermédiaires financiers à identifier les membres d'une organisation criminelle présumée au sens de l'art. 260ter CP est probablement due à de multiples raisons. La transformation des fonds incriminés en argent liquide pourrait jouer un rôle, tout comme le fait que les transactions restent en dessous d'un certain seuil. En outre, les sociétés signalées sont souvent actives dans des domaines qui se caractérisent par des transactions en espèces jusqu'à un certain degré (restauration, garages, etc.). Cependant, aussi d'autres secteurs (intermédiation dans le domaine immobilier, le secteur de la construction, etc.) pourrait être touchés.

Appartenance à une organisation criminelle et transactions en espèces
En 2020, un intermédiaire financier a signalé deux demandes de cartes de crédit en vertu de l'art. 9, al. 1, let. b, LBA (tentative de blanchiment d'argent), en raison d'une concordance dans World-Check concernant l'un des deux demandeurs. Selon cette donnée, la personne en question ferait partie de l'organisation criminelle N'drangheta. Les cartes de crédit des deux demandeurs devaient être alimentées par le même compte d'entreprise, un glacier. Les deux demandeurs ont indiqué être domiciliés dans un canton suisse, tandis que l'entreprise a son siège dans un canton frontalier.
Se fondant sur les informations contenues dans la communication, le MROS a pu requérir les renseignements nécessaires au sens de l'art. 11a, al. 2 et 3, LBA relatifs aux comptes bancaires des personnes physiques et à celui du glacier. À la suite de quoi l'intermédiaire financier ayant fourni ces renseignements a lui aussi déposé une communication de soupçons, se fondant notamment sur les sources publiques disponibles et sur la demande du MROS.
L'analyse par le MROS des relations bancaires examinées dresse le tableau suivant : 80 % des relations d'affaires signalées ont présenté un nombre inhabituellement élevé de versements en espèces. Tous les propriétaires des sociétés ou partenaires contractuels signalés possèdent la nationalité italienne. 80 % des relations d'affaires présentent plusieurs transactions en provenance ou à destination de l'Italie.
En examinant le modèle des transactions, le MROS a pu en outre constater que 60 % des relations d'affaires présentaient un lien avec la Calabre ou la ville de Naples en Italie.
Par ailleurs, l'analyse des documents relatifs au compte du glacier a révélé que celui-ci n'était probablement pas opérationnel. Au cours de la pandémie, le glacier a été apparemment, selon les déclarations du propriétaire, reconverti en restaurant.

Comme nous l'avons montré, il existe toutefois des facteurs qui, cumulés, peuvent être un signe que des fonds incriminés transitent par une relation d'affaires. La conjugaison de trois éléments en particulier – des transactions en espèces, des sociétés qui ne sont pas actives et un lien avec certains facteurs de risque (comme dans l'exemple ci-dessus le lien avec la Calabre en Italie) – peut servir de signal pour enquêter sur les comptes de membres potentiels d'une organisation criminelle.

5.3 Financement du terrorisme

L'attrait des crypto-monnaies pour le financement du terrorisme
Un intermédiaire financier met le service Crypto ATM à la disposition de ses clients. Ce service permet de verser des francs suisses dans un bancomat qui sont ensuite changés en bitcoins par l'intermédiaire financier prestataire. Pour l'échange de francs suisses en bitcoins, cet intermédiaire financier collabore avec une bourse de crypto-monnaies du sud de l'Europe. Cette bourse a porté à l'attention de l'intermédiaire financier une transaction de 0.00897707 BTC (100 CHF), effectuée de Suisse vers une adresse bitcoin qui serait attribuée au groupe Al-Qaïda. Cette adresse bitcoin aurait fait l'objet d'instructions d'un ministère public dans un pays tiers.
La personne signalée au MROS a pu garder l'anonymat en effectuant son versement au Crypto ATM puisqu'elle n'a dû indiquer qu'une donnée de contact. Le MROS a néanmoins pu identifier cette personne sur la base de cette indication. Les clarifications ont révélé que cette personne s'était déjà fait remarquer sur les réseaux sociaux il y a quatre ans en partageant de la propagande djihadiste violente.
Outre la transaction susmentionnée, 17 autres transactions ont été identifiées à la même adresse bitcoin, pour une valeur totale de près de 3000 CHF, dans le cadre de l'analyse des transactions. Cette adresse appartiendrait à l'al Qaeda Bitcoin Transfer Office selon un outil d'analyse de la chaîne de blocs.

Comme l'illustre le cas d'espèce, les groupes terroristes utilisent eux aussi les nouvelles technologies pour leur financement. La surveillance et la poursuite ultérieure de crypto-transactions ainsi que les clarifications y relatives au sens de l'art. 6 al. 2 LBA constituent une tâche importante des intermédiaires financiers. Cet exemple montre en outre que l'indication d'une simple donnée de contact était décisive pour que le MROS puisse identifier les liens nécessaires.

Focalisation sur les renseignements concernant les auteurs et les destinataires de transfert de fonds plutôt que sur les montants
Un intermédiaire financier autorisé à exercer en Suisse reçoit, par le biais de sa maison mère à l'étranger, des informations d'une autorité de poursuite pénale étrangère, selon lesquelles certaines personnes auraient effectué des transactions suspectes aux fins de financement du terrorisme via l'intermédiaire financier. Le travail du MROS a été grandement facilité par l'analyse bien documentée des transactions et des personnes impliquées faite par l'intermédiaire financier. Dans la communication, les destinataires étaient également nommés, ce qui a fourni des éléments de référence supplémentaires au MROS. Il est apparu que deux personnes issues du milieu islamiste enclin à la violence, dont l'une a un lien de parenté avec un foreign terrorist fighter suisse, ont viré des montants de plusieurs centaines voire plusieurs milliers de francs notamment vers deux pays du sud-est de l'Europe, mais aussi vers un pays asiatique, où le frère de l'une d'entre elles a réceptionné l'argent. Selon des sources médiatiques publiques, un autre destinataire de ces montants avait déjà séjourné dans un pays sensible et a été condamné par un tribunal à son retour.

Ce schéma de transaction est caractéristique des deux formes de financement du terrorisme au sens du GAFI[24], qui se produisent aussi en Suisse depuis plusieurs années, mais qui restent souvent non détectées. L'une d'entre elles concerne le transfert de fonds d'un pays à des extrémistes parfois même connus médiatiquement, qui utilisent cet argent pour leur entretien dans le pays destinataire ou qui le transfèrent parfois plus loin en vue de la planification d'attentats. La seconde forme reconnaissable dans le cas d'espèce est la suivante : des fonds pouvant potentiellement servir à des attentats à motivation extrémiste transitent par plusieurs pays successifs afin de masquer l'origine de la source du financement. Dans cette chaîne de transferts, la Suisse fait office de point de départ ou seulement de station intermédiaire. En raison des montants très bas qui n'éveillent pas de soupçons dans le cadre de transferts par des prestataires de services de paiement ou à partir de comptes privés (*retail*), de tels virements sont difficiles à déceler. Cela est principalement dû au fait que, lorsqu'on surveille des transactions, on se concentre souvent sur le montant des fonds virés. Si ce principe fonctionne bien pour mettre au jour les flux de transactions dans le cadre d'actes présumés de blanchiment d'argent, en revanche, il n'est pas idéal pour déceler le financement du terrorisme. Pour ce faire, ce sont plutôt les auteurs et les destinataires de transferts de fonds qu'il faut passer à la loupe.

5.4 Traite des êtres humains

Smurfing, milieu de la prostitution, pays à risques et renseignements précis sur les destinataires de fonds
Un prestataire de services de paiement a signalé cinq relations clients distinctes en l'espace de deux mois qui présentaient des recoupements dans leur schéma de transaction et les caractéristiques démographiques (par exemple âge, sexe, origine, profession, etc.) des personnes impliquées, et comportaient en outre des indices de traite des êtres humains (art. 182 CP) et/ou d'encouragement à la prostitution (art. 195 CP).
Les cinq clientes signalées ont effectué à la même période plusieurs versements d'un

[24] Cf. la publication du GAFI *Terrorist Financing Risk Assessment Guidance.*

montant identique à diverses personnes qui réceptionnaient ces fonds dans un pays des Caraïbes et un pays européen. On peut imaginer que les versements ont été volontairement répartis de manière à ne pas dépasser la limite des 5000 CHF, afin de ne pas avoir à se soumettre à des obligations de clarification plus approfondies. On a constaté que dans une partie des versements effectués par les clientes, les destinataires concordaient. De ce fait, l'intermédiaire financier a pu établir un lien évident entre les différentes relations d'affaires. Dans un cas, les clientes signalées ont effectué un versement entre elles qui a ensuite été transféré dans le même pays caribéen.
La plupart des clientes travaillent dans le milieu de la prostitution ou entretiennent des liens avec celui-ci. À de rares exceptions près, tous les paiements ont été effectués depuis la même agence à proximité d'un célèbre quartier suisse de prostitution. L'intermédiaire financier déclarant a examiné et suivi les schémas de transaction en sortant du cadre de la relation client, ce qui lui a permis de découvrir des liens importants entre des relations d'affaires qui n'avaient à première vue aucun lien entre elles.

Grâce au fait que l'intermédiaire financier a transmis le nom, le prénom, la date de naissance et l'adresse de toutes les personnes concernées, le MROS a pu mener des recherches approfondies et ciblées sur elles, et identifier ainsi divers éléments confirmant les soupçons de l'intermédiaire financier. Les renseignements détaillés sur les destinataires à l'étranger ont notamment permis au MROS d'adresser des demandes ciblées à des bureaux de communication étrangers – une mesure qui peut être essentielle pour des crimes transnationaux tels que la traite des êtres humains.
Dans le cas d'espèce, deux clientes ont indiqué des adresses qui se trouvent dans un quartier de prostitution. Parmi les autres adresses indiquées par les clientes, deux sont fausses, ce qui a fourni un indice supplémentaire laissant penser que les transferts effectués pouvaient être d'origine criminelle. Les pays d'origine des victimes potentielles et la nationalité de certaines des cocontractantes sont considérés, combinés à d'autres facteurs, comme des pays à haut risque. L'intermédiaire financier déclarant se réfère dans son analyse à différents indicateurs qui, selon le rapport de l'Organisation pour la sécurité et la coopération en Europe (OSCE) paru en 2019 *Following the Money : Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings*[25], sont révélateurs de possibles activités et actes dans le domaine de la traite des êtres humains :

- l'utilisation d'adresses situées dans des quartiers rouges ou des bâtiments où l'on s'adonne notoirement au commerce du sexe ;
- le recours à des hommes de paille ;
- l'utilisation d'instituts qui ne font pas partie du système financier traditionnel ;
- des transferts de différentes régions aux mêmes personnes dans des pays connus pour présenter un risque accru de traite des êtres humains ;
- des transferts structurés *(smurfing);*
- des paiements importants et/ou fréquents [...], qui ne sont pas compatibles avec l'usage personnel ou l'activité commerciale indiquée par la personne (l'argent est utilisé par un tiers).

Concernant la liste complète des divers indicateurs compilés par le représentant spécial et coordinateur de la lutte contre la traite des êtres humains de l'OSCE ainsi que les outils d'analyse financière dans le domaine de la traite des êtres humains, nous renvoyons à ladite publication de l'OSCE.

[25] Cf. la publication de l'OSCE disponible sur le site internet suivant : https://www.osce.org/cthb/438323 (document en anglais).

5.5 Communications en lien avec des fournisseurs de services d'actifs virtuels (VASP)

Des escrocs adeptes du phishing utilisent une bourse de crypto-monnaies suisse pour blanchir des valeurs patrimoniales acquises frauduleusement

Un intermédiaire financier a signalé le compte commercial d'une bourse de crypto-monnaies suisse, sur lequel sont entrés en quelques jours environ 30 000 CHF de fonds de clients de diverses banques. Les clients de ces instituts financiers ont été poussés à dévoiler leurs données d'accès personnelles de e-banking (phishing) par de faux e-mails. Les ordres de paiement correspondants ont ensuite été émis par des tiers inconnus. Les instituts financiers dont les clients ont été touchés par des attaques de phishing ont alerté l'intermédiaire financier déclarant à propos des fonds incriminés. De son côté, la bourse de crypto-monnaies suisse a signalé au MROS l'achat de bitcoins sur sa plate-forme commerciale au moyen des fonds en question. Elle a transmis les adresses bitcoin concernées au MROS ainsi que les adresses IP des auteurs présumés qui ont émis les ordres d'achat. Ces transactions ont été effectuées via une interface de programmation d'application, ou API (Application Programming Interface), que la bourse de crypto-monnaies met à la disposition de ses clients sur son site Internet. L'API sert d'interface avec la plate-forme commerciale de la bourse et permet aux cliens d'effectuer des transactions d'achat et de vente simplifiées et automatisées jusqu'à 5000 CHF par jour, sans que les clients doivent fournir des renseignements détaillés sur leur identité lors de leur enregistrement. Lors de transactions d'achat et de vente via son API, la bourse demande au client de lui indiquer uniquement un compte de provenance des fonds, qui est normalement sous le contrôle du donneur d'ordre légitime, ainsi qu'une adresse de crypto-monnaies, sur laquelle les crypto-monnaies achetées seront virées. Au moment de terminer un ordre d'achat généré à travers l'interface, les clients reçoivent un numéro de référence qu'ils doivent indiquer lors du virement bancaire sur le compte commercial de la bourse. Du fait que tous les ordres d'achat effectués étaient d'une valeur de 5000 CHF ou très légèrement inférieure (technique du smurfing ou fractionnement), la bourse de crypto-monnaies n'a pas exigé d'autres documents de type Know your Customer (KYC) de la part des donneurs d'ordre.

Des crypto-actifs acquis frauduleusement sont blanchis sur une bourse de crypto-monnaies suisse

En 2019 a eu lieu une cyberattaque contre une bourse de crypto-monnaies étrangère, lors de laquelle des valeurs patrimoniales s'élevant à plusieurs millions de francs suisses ont été volées sous la forme de la crypto-monnaie « F ». On suppose que les auteurs présumés font partie d'un groupe de pirates informatiques. Pour effacer leurs traces, les pirates ont changé les crypto-actifs volés en bitcoins (chain-hopping, soit le passage de la chaîne de blocs « F » à la chaîne de blocs bitcoin, ce qui complique la traçabilité au moyen du logiciel de traçage). Ils ont manifestement sélectionné de façon ciblée des bourses de crypto-monnaies dans le monde qui appliquent une procédure d'identification simplifiée des clients pour un échange de ce type, c'est-à-dire qu'elles exigent uniquement une adresse e-mail ou un numéro de téléphone lors de l'enregistrement du client, pour autant que les valeurs patrimoniales échangées ne dépassent pas un certain montant limite. Les criminels ont subdivisé la quantité de « F » volée en petits montants qu'ils ont fait transiter par d'innombrables adresses « F » (hops), avant de les déposer sur les différentes bourses de crypto-monnaies pour l'échange. De cette manière, ils ont réussi à la fois à rendre le traçage plus difficile et à contourner les systèmes d'alerte précoce des bourses de

crypto-monnaies, de sorte qu'il n'était plus directement apparent qu'il s'agissait des crypto-actifs volés lors de la cyberattaque. Dans ce cas aussi, l'interface API d'une bourse de crypto-monnaies suisse déjà mentionnée a été utilisée abusivement. Les auteurs ont ouvert plusieurs comptes dans ladite bourse et ont changé les unités volées de crypto-monnaie « F » en bitcoins, en veillant à ne pas dépasser la contre-valeur de 5000 CHF pour ne pas avoir à remplir les exigences KYC plus approfondies. La bourse de crypto-monnaies s'est donc retrouvée en possession des unités détournées de crypto-monnaie « F », dont les traces, malgré tous les efforts des pirates, ont pu être retrouvées sur la chaîne de blocs concernée par le logiciel de traçage, et ont permis de remonter jusqu'à la cyberattaque de la place boursière de crypto-monnaies étrangère. Sur la chaîne de blocs bitcoin, les bitcoins que la bourse a viré aux cybercriminels dans l'opération de change ne présentent toutefois pas de lien avec l'attaque de la place boursière étrangère, mais uniquement un lien avec la bourse suisse. Après la découverte de cet abus, la bourse de crypto-monnaies suisse concernée a pu interrompre plusieurs transactions sortantes en bitcoins et a signalé l'incident au MROS.

En 2019, le nombre de bourses de crypto-monnaies piratées a atteint un record.[26] Du fait que les crypto-monnaies (par ex. bitcoins) peuvent être transférées directement entre l'expéditeur et le destinataire partout dans le monde et de manière relativement anonyme, l'endroit où une bourse est piratée importe peu, puisque les crypto-monnaies incriminées peuvent atterrir sur une autre place financière en l'espace de quelques secondes et y être blanchies.
Ces deux cas montrent l'importance du *smurfing* et du contournement des obligations d'identification[27] liées aux VASP. Pour éviter de tels incidents, l'utilisation d'un logiciel de traçage s'impose, qui permet de retracer les transactions. Les pirates tentent pour leur part de contourner ces systèmes d'alerte précoce en faisant transiter les crypto-monnaies d'origine criminelle par plusieurs adresses de crypto-monnaies, avant qu'elles ne parviennent à leur adresse de destination finale. Une adresse de crypto-monnaies dans une telle chaîne de transactions ne représente donc qu'une station intermédiaire (*hop*). Un traçage efficace exige donc de retracer les transactions sur plusieurs *hops*.
Ces exemples montrent une fois de plus l'importance que revêtent les outils d'analyse de traçage en matière de transactions de crypto-monnaies. Afin que le MROS puisse mobiliser ses propres moyens d'analyse, il doit pouvoir s'appuyer sur les clarifications au sens de l'art. 6 LBA documentées par les intermédiaires financiers et sur l'analyse y liée portant sur le suivi des crypto-transactions (art. 3, al. 1, let. h, OBCBA).

5.6 Identification par vidéo et en ligne

En mars 2016, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a publié la circulaire 2016/7 relative aux obligations de diligence des intermédiaires financiers qui lui sont soumis lors de l'établissement de relations d'affaires par le biais de canaux numériques. En 2018[28] – suite aux évolutions technologiques – la circulaire sur l'Identification par vidéo et en ligne a été partiellement révisée et, en 2020, la FINMA a proposé d'autres modifications qui ont fait l'objet jusqu'au 1er février 2021 d'une audition.[29] La pos-

[26] Cf. la publication de janvier 2020 de Chainalysis *The 2020 State of Crypto Crime.* Le nombre de piratages de bourses de crypto-monnaies n'a jamais été aussi élevé qu'en 2019 (Chainalysis dénombre 11 piratages), le total du butin étant toutefois plus petit que les années précédentes (2019 : 282,6 millions USD ; 2018 : 875,5 millions USD ; 2014 : 483,1 millions USD).

[27] On relèvera toutefois qu'avec l'entrée en vigueur le 1er janvier 2021 de l'art. 51a Ordonnance de la FINMA sur le blanchiment d'argent du 3 juin 2015 (OBA-FINMA, RS **955.033.0**), la valeur seuil pour les opérations de change en crypto-monnaies a été abaissée de 5000 CHF à 1000 CHF, ce qui correspond à une mise en œuvre de la note interprétative de la recommandation 15 du GAFI, relative à la gestion des VASP publiée à la mi-2019. Ces règles ont été reprises par les OAR qui comptent des prestataires de cryptomonnaies parmi leurs affiliés.

[28] Cf. communiqué de presse www.finma.ch/fr/news/2018/07/20180717-mm-video-online-id/.

[29] Cf. communiqué de presse www.finma.ch/fr/news/2020/11/20201116-mm-online-identifizierung/

sibilité d'établir une relation d'affaires de cette manière est désormais offerte par la plupart des établissements bancaires helvétiques. Certains intermédiaires financiers, en particulier ceux actifs dans le commerce de monnaies virtuelles, y recourent désormais de façon systématique. Le nombre de cas signalés au MROS par des intermédiaires financiers dont les soupçons ont été éveillés lors du processus d'identification en ligne de leurs clients au moment de l'ouverture d'une relation d'affaires par voie numérique sont par conséquent de plus en plus fréquents. Près des deux tiers de ceux-ci se rapportent à l'usage de crypto-monnaies. Un des grands cas annoncé par le passé concernait par exemple l'identification en ligne d'investisseurs potentiels dans le cadre d'une *Initial Coin Offering.*[30]

L'établissement de relations d'affaires par le biais de canaux numériques n'est en effet pas exempt de risques. Deux possibilités principales s'offrent aux criminels désireux d'ouvrir ainsi des relations d'affaires pour y blanchir leurs fonds mal acquis : ils peuvent recourir à des faux documents d'identité ou à des documents d'identité usurpés, souvent volés.[31] Ces deux cas de figure apparaissent souvent dans les communications de soupçons reçues par le MROS, avec une prédominance des signalements effectués à la suite de l'identification de documents falsifiés, probablement parce qu'ils sont plus aisément repérables que les documents volés. Ainsi, le MROS a reçu en 2020 une communication d'un intermédiaire financier offrant la possibilité d'ouvrir des comptes en ligne après un processus d'identification par la soumission de copies de documents d'identité par Internet. Ses soupçons ont été éveillés par des informations négatives de sources ouvertes qui accusaient les clients de pratiquer une escroquerie aux investisseurs dans le cadre du lancement d'une innovation technologique. En effectuant les recherches à propos de ce cas, le MROS a pu établir que la carte d'identité utilisée par l'un des détenteurs de contrôle d'une des sociétés titulaires d'un compte signalé par l'intermédiaire financier avait fait l'objet d'une déclaration de vol trois jours avant l'ouverture du compte.

Dans la mesure où, précisément, le recours à des documents falsifiés ou usurpés lors de l'ouverture d'une relation d'affaires en ligne ne permet pas d'identifier les détenteurs de contrôle ou ayants droit économiques réels des relations d'affaires, il est particulièrement difficile de rapporter les valeurs patrimoniales faisant l'objet de soupçons à des infractions préalables au blanchiment d'argent. La collaboration du MROS avec les autorités de police suisses et avec ses homologues étrangers s'avère alors déterminante, mais la précision des informations fournies par l'intermédiaire financier déclarant augure de son efficacité.

Rupture des négociations

Un intermédiaire financier actif dans le commerce de monnaies virtuelles reçoit le même jour trois demandes d'ouverture de compte sur sa plate-forme informatique. Il remarque que dans les trois cas, le document d'identité étranger fourni par les clients potentiels présente la même photographie, avec des informations différentes relatives au nom et à la date de naissance. L'intermédiaire financier rompt alors les négociations d'ouverture de relation d'affaires et effectue de plus amples vérifications sur les comptes de ses clients récents, en communiquant ses soupçons au MROS au sens de l'art. 9, al. 1, let. b, LBA (tentative de blanchiment d'argent). Cela lui permet d'identifier trois autres clients dont les documents d'identité présentent la même photographie. Ces relations d'affaires sont dès lors signalées au MROS. L'analyse du MROS permet d'identifier les comptes étrangers à partir desquels les trois clients déjà acceptés ont crédité le compte de l'intermédiaire financier pour acheter des crypto-monnaies. Grâce aux informations reçues de la CRF du pays d'où ces virements ont été effectués, le MROS peut confirmer

[30] Méthode de levée de fonds, fonctionnant via l'émission d'actifs numériques échangeables contre des crypto-monnaies ou des monnaies fiat durant la phase de démarrage d'un projet.

[31] Cf. la publication du GAFI *Guidance on digital identity,* publiée en mars 2020.

que les fonds transférés pour acheter des crypto-monnaies proviennent d'escroqueries commises à l'étranger. En outre, grâce aux informations fournies par l'intermédiaire financier déclarant, il est en mesure de transmettre à son homologue étranger les adresses IP des ordinateurs depuis lesquels les virements ont été effectués, ce qui permet à l'homologue étranger concerné de dénoncer les auteurs des escroqueries et du blanchiment d'argent subséquent aux autorités de poursuite pénale compétentes.

Conformément aux recommandations du GAFI, plusieurs intermédiaires financiers confrontés aux risques découlant des processus d'identification en ligne semblent avoir amélioré ceux-ci. Abandonnant les vérifications auxquelles les personnes chargées de la conformité procédaient manuellement, ils ont désormais recours à des programmes informatiques de contrôle de l'authenticité des documents présentés, qui présentent une plus grande fiabilité.
Par ailleurs, nous constatons relativement peu de communications effectuées suite à une rupture des négociations visant à l'ouverture d'une relation d'affaires. L'usage de fausses pièces de légitimation pourrait, à notre sens, amener à des signalements faits sur la base de l'art. 9, al. 1, let. b, LBA.

6. Pratique du Bureau de communication

6.1 Transmission d'informations – et pas de communications

Avec l'adaptation de l'OBCBA entrée en vigueur le 1er janvier 2020, les communications de soupçons ne sont plus transmises aux Ministères publics. Afin de garantir la protection des sources – aucune indication relative à l'auteur de la communication ou à la personne ayant communiqué des informations n'est transmise aux autorités de poursuite pénale (cf. art. 8, al. 1, OBCBA). Les informations pertinentes et l'évaluation que le MROS en fait sont adressées aux Ministères publics sous forme de rapports électroniques. Les dénonciations destinées aux autorités de poursuite pénale peuvent contenir des informations provenant de différentes sources ou de différentes communications (cf. art. 1, al. 2, let. a-e, OBCBA). C'est la nature agrégée des informations enregistrées par le MROS qui détermine leur sort. Comme déjà évoqué (cf. ch. 4.12), la notion de « taux de transmission » des communications de soupçons n'est par conséquent plus pertinente. Le second point sur lequel il faut insister est en relation avec le premier. Lorsque le traitement des informations provenant d'une communication de soupçons est terminé, le MROS signale aux intermédiaires financiers, en relation avec l'art. 23, al. 5 et 6, LBA, si les informations communiquées ont été transmises ou non. Cette information n'a que deux fonctions pratiques : en cas de transmission, elle oblige les intermédiaires financiers à bloquer les avoirs des relations signalées conformément aux dispositions de l'art. 10 LBA. En cas d'une décision de non transmission à une autorité de poursuite pénale, elle permet aux intermédiaires financiers de décider de leur propre chef de l'opportunité de poursuivre la relation d'affaires signalée, conformément aux dispositions de l'art. 30 de l'OBA-FINMA. Comme par le passé, ces décisions ne permettent en aucun cas de tirer des conclusions sur la licéité des avoirs entreposés sur les relations d'affaires signalées. Des décisions de non transmission de la part du MROS peuvent très bien intervenir après des transmissions d'informations à des CRF homologues ou à une autorité administrative nationale, ou encore parce que les informations importantes provenant de la communication ont été signalées dans un rapport sans que la transmission de l'ensemble des informations de la communication ne soit justifiée.

6.2 Nouvelles compétences en lien avec l'art. 11a, al. 2bis, LBA

6.2.1 Le nouvel art. 11a, al. 2bis, LBA

Le 25 septembre 2020, le Parlement a accepté l'« arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé ».[32] Cet arrêté modifie la LBA, en y introduisant notamment un nouvel art. 11a, al. 2bis, formulé ainsi :

[32] FF **2020** 7651, 7664.

« 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 ».

Le 31 mars 2021, le Conseil fédéral a décrété que ces nouvelles dispositions entreraient en vigueur le 1er juillet 2021.[33]
Dès son entrée en vigueur, cette modification de la LBA confèrera au MROS de nouvelles compétences en matière de lutte contre le blanchiment d'argent, les infractions préalables au blanchiment d'argent, la criminalité organisée ou le financement du terrorisme. Depuis le 1er novembre 2013, le MROS dispose de la possibilité sur la base d'une analyse transactionnelle de solliciter auprès d'intermédiaires financiers helvétiques des informations supplémentaires nécessaires à ses analyses, en relation avec des comptes tiers avec lesquels des transactions auraient été effectuées depuis la relation d'affaires signalée. Le but du législateur était de donner au MROS des moyens supplémentaires pour approfondir ses analyses et suivre, à certaines conditions, le *paper trail*. En quelques années, cette disposition est devenue cardinale pour le MROS.
L'usage des demandes d'informations supplémentaires au titre de l'article 11a LBA, couplée à la possibilité pour le MROS d'échanger des informations avec ses homologues étrangers et d'autres autorités nationales, ont en effet permis d'améliorer les analyses du MROS et d'éviter de surcharger les autorités de poursuite pénale. Jusqu'à présent, les demandes effectuées au titre de l'article 11a LBA étaient toutefois limitées à l'analyse des cas dans lesquels le MROS disposait déjà d'une communication de soupçons effectuée par un intermédiaire financier suisse. Par conséquent, le MROS ne pouvait effectuer de telles requêtes portant sur l'analyse des demandes provenant de CRF homologues que dans la mesure où celles-ci étaient en relation avec des informations financières annoncées au MROS par un intermédiaire financier suisse. Si celles-ci révélaient un lien de connexité avec une communication, le MROS était en mesure d'y répondre. Dans le cas contraire, le Bureau de communication ne pouvait donner d'informations financières à la CRF requérante.
Cette lacune a été critiquée lors de l'évaluation de la Suisse par le GAFI, survenue en 2016. De ce fait, la Suisse n'a été jugée que « partiellement conforme » (une notation insuffisante) à la recommandation 40 du GAFI et le niveau d'efficacité atteint par la Suisse au niveau de la coopération internationale (RI 2) n'a été jugé que « modéré », une notation également insuffisante.[34] La correction de cette défaillance importante faisait par conséquent partie des huit actions prioritaires demandées à la Suisse par les évaluateurs. Ceci était justifié entre autres eu égard à la forte internationalisation de la place financière suisse.
Cette évaluation insatisfaisante de la Suisse a également déclenché une procédure de conformité à l'encontre du MROS au sein du groupe Egmont, le forum d'échange opérationnel pour les CRF. Aux termes des règles gouvernant l'application des principes de ce groupe, le MROS fait l'objet d'un processus de suivi et doit rendre compte des mesures prises pour répondre aux insuffisances relevées par l'évaluation du GAFI. Si le dispositif légal helvétique n'était pas adapté dans un certain délai pour y pallier, le MROS risquerait d'être suspendu du groupe Egmont. Rappelons que des liens d'extranéité sont relevés dans une majorité des communications de soupçons qui parviennent au MROS et que, dans de tels cas, la possibilité pour le Bureau de communication de recourir aux informations dont disposent les CRF du groupe Egmont est essentielle. Les nouvelles dispositions de l'art. 11a, al. 2bis, LBA devraient permettre de satisfaire aux standards internationaux et de mettre un

[33] Cf. le communiqué de presse *Lutte contre le terrorisme : entrée en vigueur de dispositions pénales renforcées.*

[34] Cf. *mer-suisse-2016.pdf (fatf-gafi.org).*

terme à la procédure de suivi dont le MROS fait l'objet au sein du groupe Egmont.
À l'avenir, et grâce aux nouvelles dispositions de l'art. 11a, al. 2bis LBA, le MROS sera en effet en mesure de requérir des intermédiaires financiers des informations sur une ou plusieurs transactions ou une relation d'affaires signalée par une autre CRF, par exemple par une information spontanée, ou faisant l'objet d'une demande d'un homologue étranger même en l'absence d'une communication de soupçons d'un intermédiaire financier suisse. Cette compétence étendue profitera également aux intermédiaires financiers helvétiques, dans la mesure où elle permettra d'attirer leur attention sur des risques potentiels présents dans leurs livres et ignorés jusqu'alors et d'augmenter par conséquence la sécurité en Suisse. Cette amélioration dans l'échange d'informations (*financial intelligence*) entre CRF permettra de soutenir l'entraide internationale et la poursuite pénale.

6.2.2 L'échange d'informations avec les homologues étrangers

L'entraide administrative internationale entre le MROS et ses homologues étrangers est réglée par les art. 30 et 31 LBA. Le MROS échangera par conséquent avec ses homologues étrangers les informations financières obtenues par le nouvel art. 11a, al. 2bis, LBA aux conditions qui ont prévalu jusqu'ici. Le Conseil fédéral a eu l'occasion de se prononcer à plusieurs reprises à ce sujet.[35] Rappelons qu'avant d'échanger des informations avec une CRF étrangère, le MROS vérifie tout d'abord le respect des conditions de l'art. 30 LBA. Il s'agit entre autres de l'application du principe de spécialité, de la réciprocité et du respect du secret de fonction. Les demandes des homologues étrangers doivent ensuite répondre aux exigences de l'art. 31 LBA. Ainsi, le MROS n'accepte pas d'entrer en matière pour les demandes qui ne présentent manifestement pas de lien avec la Suisse (*fishing expeditions*). Il ne répond pas non plus aux requêtes qui visent à contourner la voie de l'entraide internationale en matière pénale. Enfin, le Bureau de communication ne fournit pas d'informations dans les cas où les intérêts nationaux ou la sécurité et l'ordre public suisses pourraient être compromis. Les informations obtenues ne peuvent être utilisées par la CRF qui les reçoit que dans le cadre de ses analyses se référant au blanchiment d'argent, à ses infractions préalables, à la criminalité organisée et au financement du terrorisme. Sur autorisation préalable du MROS, les informations transmises à une CRF étrangère peuvent aussi être communiquées aux autorités tierces du même pays. Pour donner cette autorisation, le MROS vérifie l'application des conditions de l'art. 30, al. 4 et 5, LBA. Rappelons que les informations transmises ne peuvent être utilisées qu'à titre de renseignement (*intelligence*) et non comme moyens de preuve, et qu'elles ne sont transmises que sous forme de rapport (art. 30, al. 3, LBA).

6.2.3 Les premières questions pratiques d'application du nouvel art. 11a, al. 2bis, LBA

L'entrée en vigueur de cette nouvelle disposition légale pose quelques questions pratiques d'application pour les intermédiaires financiers, qui méritent d'être relevées ici. Les règles auxquelles les intermédiaires financiers devront se conformer lorsqu'ils recevront une demande de remise d'informations basée sur le nouvel art. 11a, al. 2bis et 3, LBA sont identiques aux règles éprouvées adoptées depuis 2013 au sujet des demandes fondées sur l'art. 11a al. 2 LBA.[36] Afin d'obtenir des informations supplémentaires, le MROS utilise des formulaires adaptés conformément à l'art. 11a, al. 1 ou al. 2, LBA. Une liste de documents/informations à remettre y est prévue. Le MROS sélectionne ceux qui sont pertinents selon la base légale correspondante (art. 11, al. 1, ou art. 11a, al. 2 ou 2bis, LBA). Le contenu du formulaire

---

35 Cf. par exemple le message relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé du 14 septembre 2018, FF **2018**, 6541 ss ainsi que le message du 27 juin 2012 relatif à la modification de la loi sur le blanchiment d'argent, FF **2012** 6449, 6487 ss.

36 À ce sujet, voir le *rapport annuel 2013 du MROS,* pp. 56 ss.

utilisé pour les demandes basées sur l'art. 11a, al. 2bis, sera identique à celui qui est utilisé pour les demandes basées sur l'art. 11a, al. 2, LBA. Les intermédiaires inscrits dans goAML recevront de telles demandes d'informations et seront priés d'y répondre par ce canal en se basant sur la pratique documentée dans le manuel qui leur est destiné.[37]
Rappelons que cette demande ne doit pas provoquer une communication de soupçons automatique au MROS. L'intermédiaire financier qui reçoit une telle demande doit y répondre. Il ne peut toutefois pas ignorer le fait qu'il s'agit d'une demande d'une autorité basée sur des soupçons de blanchiment d'argent, d'infractions préalables au blanchiment d'argent, de criminalité organisée ou de financement du terrorisme. L'intermédiaire financier doit donc effectuer des clarifications supplémentaires en vertu de l'art. 6 LBA et, en cas de soupçons simples ou fondés, communiquer le cas au MROS. Si aucun soupçon ne se concrétise, l'intermédiaire financier se contentera de transmettre au MROS les informations demandées en vertu de l'art. 11a al. 2bis LBA et de documenter ces clarifications (cf. art. 7 LBA et art. 31 OBA-FINMA).
Comme par le passé, lorsqu'il se trouve dans le premier cas de figure, l'intermédiaire financier qui déciderait de signaler la relation faisant l'objet d'une demande de renseignements du MROS peut s'acquitter de celle-ci en annexant les documents requis et les informations demandées à sa communication de soupçons, tant que celle-ci est effectuée dans le délai imparti pour répondre à la demande du MROS. Ce délai est fixé par le MROS conformément à l'art. 11a, al. 3, LBA. L'intermédiaire financier requis mettra à disposition du MROS les informations dont il dispose. Comme le Conseil fédéral l'a précisé, dans le cadre de l'art. 11a LBA, « sont considérées comme disponibles toutes les informations qui sont en possession des entités d'une entreprise ou qui peuvent être acquises, pour autant que ces entités relèvent de la juridiction suisse ».[38]

6.3 Ordonnance de production de pièces des autorités de poursuite pénale et obligation de communiquer

Est-il nécessaire de procéder à une communication de soupçons dès l'instant où un séquestre pénal a déjà été ordonné par une autorité de poursuite pénale ? Cette question est posée au MROS de façon récurrente par les intermédiaires financiers et/ou d'autres intéressés.
Cette question a déjà été réglée par le MROS voici plus de dix ans[39], et confirmée par la jurisprudence de 2018 du Tribunal fédéral.
Le message du Conseil fédéral concernant l'adoption de la LBA précise son sens et son but : *« La cible principale de cette lutte est le crime organisé. Il ne s'agit donc pas seulement de détecter et de confisquer les fonds incriminés, mais surtout d'établir et de conserver des documents (paper trail) et de communiquer les informations (obligation de communiquer) permettant d'identifier et de poursuivre pénalement les personnes coupables de blanchissage d'argent. »*[40]

Les dispositions de la LBA visent ainsi, en premier lieu, la répression générale du délit de blanchiment d'argent et la poursuite pénale des prévenus de ce délit. Le blocage et le séquestre des valeurs patrimoniales potentiellement incriminées est un élément, certes, qui n'est pas indifférent mais il ne revêt ni un caractère exclusif, ni prépondérant. Il sied donc de souligner que les objectifs de la LBA ne sont pas alternatifs. La réalisation du premier objectif n'implique pas nécessairement la réalisation du deuxième ou autrement dit, les deux finalités indiquées sont indépendantes et doivent être atteintes, certes autant que possible, de façon coordonnée.

---

37 Cf. la publication *goAML Web – Manuel d'utilisation,* pp. 22 et 47.

38 FF **2018** 6469, 6543.

39 Cf. le ch. 5.5 « Ordonnance de production de pièces des autorités de poursuite pénale et obligation de communiquer » du *rapport annuel 2007 du MROS,* pp. 88 ss et le ch. 4.1 du *rapport annuel 2017 du MROS* (p. 57) où la pratique publiée en 2007 a été confirmée. Voir aussi la pratique du MROS publiée au même endroit : *Publications du Bureau de communication en matière de blanchiment d'argent (MROS).*

40 FF **1996** III 1057, 1072.

Le MROS a intégré dès 2007 la finalité de la LBA dans sa pratique administrative concernant l'obligation de communiquer des intermédiaires financiers en cas de réception d'une ordonnance de perquisition et/ou de séquestre. À l'époque, le MROS avait souligné que cette question ne devait pas être tranchée de manière définitive. Elle doit être appréciée au cas par cas, en prenant en considération les résultats des clarifications complémentaires que l'intermédiaire financier est appelé à devoir mettre en œuvre dans de pareils cas en application de l'art. 6, al. 2, LBA en liaison avec les art. 15 et suivants de l' OBA-FINMA : « en principe, une ordonnance de production des pièces ou de décision de séquestre implique toujours l'obligation particulière de clarification ».[41]

Si les résultats des clarifications complémentaires déclenchées par la réception d'une ordonnance de perquisition et/ou de séquestre permettent à l'intermédiaire financier d'identifier des éléments de soupçons supplémentaires, tant ou niveau transactionnel qu'au niveau de la relation d'affaires et que ces éléments de soupçons lui permettent de former un soupçon fondé au sens de l'art. 9, al. 1, let. a, LBA, il doit alors adresser une communication de soupçons au MROS. Tel est le cas, par exemple, lorsque les clarifications complémentaires mènent à l'identification d'autres relations d'affaires que celles visées par l'ordonnance de perquisition et/ou de séquestre réceptionnée. L'intermédiaire financier peut tomber sur des personnes mentionnées dans l'ordonnance qui sont impliquées en tant que titulaires, ayants droit économiques, ayants droit de signature, détenteurs de contrôle ou donneurs d'ordre et bénéficiaires de virements internes ou internationaux. L'intermédiaire financier doit aboutir au même résultat et communiquer lorsque l'analyse transactionnelle de la relation d'affaires frappée par l'ordonnance de production des pièces et/ou de séquestre indique l'existence de transactions suspectes en dehors du laps de temps indiqué par le Ministère public. Nous rappelons, d'ailleurs, que l'intermédiaire financier n'est pas lié par les circonstances de fait, généralement succinctes, indiquées par l'autorité de poursuite pénale responsable de l'ordonnance de perquisition et/ou de séquestre.

Cela implique que, si dans le cadre des clarifications complémentaires au sens de l'art. 6, al. 2, LBA en liaison avec les art. 15 ss OBA-FINMA, l'intermédiaire financier devait détecter des éléments de soupçons supplémentaires ou nouveaux en lien avec les mêmes ou d'autres personnes mentionnées dans l'ordonnance de production des pièces et/ou de séquestre ou impliquées dans la relation d'affaires dont les valeurs patrimoniales sont objet du séquestre ou dans d'autres relations d'affaires et pour des nouveaux éléments pouvant fonder un soupçon, l'intermédiaire financier est également obligé de communiquer en application de l'art. 9, al. 1, let. a, LBA. Dans ces cas, l'intermédiaire financier doit toujours annexer à la communication, l'ordonnance de production des pièces et/ou de séquestre concernée (art 3, al. 1, let h OBCBA).[42]Le MROS exerce dans ces cas une activité de vérification et de coordination avec les autorités de poursuite pénale compétentes qui permet d'évaluer les informations reçues et de décider si une transmission des informations communiquées aux autorités compétentes s'impose. Durant l'année 2020, par exemple, dans 9.1 % des cas les intermédiaires financiers ayant communiqué ont déclaré des « informations des autorités de poursuite pénale » comme raison du soupçon. Dans la majorité des cas, ces informations sont transmises par le MROS aux autorités de poursuite pénale en charge, parce qu'elles amènent des informations nouvelles, jugées utiles pour la conduite de la procédure pénale en cours.

En revanche, si l'obligation de clarification de l'intermédiaire financier ne permet d'apporter rien de plus que ce que l'autorité de poursuite pénale exige par le biais de l'ordonnance de production de pièces ou par la décision de séquestre, alors l'intermédiaire financier peut renoncer à adresser une communication de soupçons supplé-

41 Cf. *rapport annuel 2007* du MROS, p. 88.

42 Cf. *rapport annuel 2017* du MROS (p. 57) ainsi que *les commentaires sur la révision partielle de l'OBCBA* du 24 novembre 2019, p. 14 note 37.

mentaire au MROS. En effet, une telle communication constituerait un doublon inutile.
Ceci s'applique aussi à l'intermédiaire financier tiers (gestionnaire de fortune, fiduciaire, etc.) qui a été informé par une banque sur l'existence d'une obligation de dépôt en vertu de l'art. 265 Code de procédure pénale du 5 octobre 2007[43] (après l'expiration d'une éventuelle interdiction d'informer toute personne), ou – aux conditions de l'art. 10a, al. 3, LBA – du fait qu'une communication de soupçons en vertu de l'art. 9 LBA a été effectuée.
Selon la jurisprudence du Tribunal fédéral[44], l'obligation de communiquer ne prend pas fin avec la saisine de l'autorité de poursuite pénale : elle « perdure aussi longtemps que les valeurs peuvent être découvertes et confisquées ».[45]
L'ouverture d'une instruction ne signifie pas encore que les conditions pour le prononcé d'un séquestre pénal sont remplies. En revanche, la communication de l'intermédiaire financier au MROS conformément aux art. 9 LBA et 3 OBCBA peut aboutir très rapidement, sur la base de l'art. 10 LBA, au blocage provisoire des avoirs. La déclaration d'opérations suspectes est une obligation propre à l'intermédiaire financier, indépendante d'une éventuelle procédure pénale.
Or, quand l'intermédiaire financier reçoit une ordonnance de perquisition et/ou de séquestre, il s'engage, par une application correcte des obligations de diligence particulières prévues à l'art. 6, al. 2, LBA en liaison avec les art. 15 et suivants OBA-FINMA, à découvrir la totalité des valeurs patrimoniales potentiellement incriminées encore déposées en ses livres ou sur des relations d'affaires désormais clôturées et à identifier d'éventuels autres éléments de soupçon. Tant que cette activité n'est pas achevée, l'intermédiaire financier n'est pas en mesure d'exclure l'existence d'un soupçon fondé.
Une communication de soupçons au sens de l'art. 9, al. 1, LBA, suivi par une dénonciation du MROS à une autorité de poursuite pénale selon l'art. 23, al. 4, LBA et le blocage des avoirs *ex lege* en résultant (art. 10 LBA), représente ainsi le seul moyen possible pour assurer la découverte de ces valeurs, afin que l'autorité de poursuite pénale compétente puisse prononcer une nouvelle ordonnance de perquisition et de séquestre ouvrant la voie, le cas échant, à une confiscation. Cette communication permet également d'identifier et de poursuivre pénalement d'éventuelles autres personnes coupables de blanchiment d'argent.

6.4 Réception des communications de soupçons par le MROS

Le MROS reçoit régulièrement des annonces qu'il ne peut pas accepter ni traiter en tant que communications au sens de la LBA ou de la loi fédérale du 18 décembre 2015 sur le blocage et la restitution des valeurs patrimoniales d'origine illicite de personnes politiquement exposées à l'étranger (LVP)[46], du fait qu'il n'a pas la compétence à raison du lieu et de la matière.
Les déclarants peuvent être des personnes physiques ou morales qui ne sont pas soumises à la LBA, ou des instituts qui sont soumis à la LBA mais qui n'agissent pas à titre d'intermédiaire financier au sens de l'art. 2 LBA ou de personne ou institution au sens de l'art. 7 LVP.
Le MROS est le seul service en Suisse habilité à réceptionner et à traiter les communications que les intermédiaires financiers, les négociants, les autorités et les organisations au sens de la LBA émettent pour soupçons de blanchiment d'argent, d'infractions préalables au blanchiment d'argent, d'appartenance à une organisation criminelle (crime organisé) ou de financement du terrorisme. Il décide si les informations communiquées doivent être transmises à une autorité de poursuite pénale (art. 23, al. 4, LBA). Par ailleurs, le MROS réceptionne les informations de personnes et d'institutions au sens de l'art. 7, al. 1 et 2, LVP et les retransmet au Département fédéral des affaires étrangères (DFAE) et à l'Office fédéral de la justice (OFJ) (art. 7, al. 6, LVP).

---

43 RS **312.0**

44 Cf. ATF 144 IV 391, consid. 3.1 et 3.3-3.4 ; ATF 142 IV 276, consid 5.4.2

45 Cf. ATF 144 IV 391, consid. 3.1

46 RS **196.1**

Dans le cas où le MROS n'accepte pas une communication de soupçons parce qu'il n'a pas la compétence à raison du lieu et de la matière, les informations contenues dans celle-ci ne peuvent pas être traitées par le MROS ni être transmises à une autorité de poursuite pénale au sens de l'art. 23, al. 4, LBA.
En raison du principe de spécialité, le MROS ne peut accepter et traiter les communications de soupçons reçues que s'il a la compétence à raison du lieu et de la matière.
Toutes les autres personnes (physiques ou morales) non soumises à la LBA et à la LVP ayant conçu un tel soupçon sont par conséquent tenues d'adresser les éléments y relatifs directement aux autorités de poursuite pénale. Habituellement, les dénonciations se font à la police du lieu de domicile du dénonciateur.
En 2020, le MROS a reçu 140 lettres de citoyens et 8 annonces présentées comme des communications de soupçons au sens de l'art. 9 LBA ou 305ter CP, pour lesquelles il n'avait pas la compétence à raison de la matière et/ou du lieu.
Dès réception d'une annonce, le MROS vérifie sa compétence d'office, mais il ne peut examiner que sommairement si l'entité déclarante est soumise à la LBA ou non, notamment parce que la loi ne lui attribue pas la compétence de déterminer matériellement s'il y a soumission à la LBA ou non. Cette tâche incombe essentiellement à la FINMA, qui a la compétence de reconnaitre les organismes d'autorégulation (OAR) et de surveillance (OS) et qui, indirectement, est aussi compétente pour ceux-ci et pour les entités surveillées par ceux-ci. La FINMA publie sur son site le nom des institutions qui disposent d'une forme d'autorisation.[47] Selon l'art. 12 LBA, sont habilités à veiller à ce que les obligations définies dans la LBA soient respectées la FINMA, mais aussi la Commission fédérale des maisons de jeu (CFMJ), l'autorité intercantonale de surveillance et d'exécution visée à l'art. 105 de la loi du 29 septembre 2017 sur les jeux d'argent (LJAr)[48], c'est-à-dire l'autorité intercantonale de surveillance des jeux d'argent (Gespa), ainsi que les organismes d'autorégulation (OAR) reconnus et les organismes de surveillance (OS) autorisés. Les informations correspondantes sont aussi publiées sur leurs sites respectifs. En outre, le MROS peut échanger des informations en la matière avec la FINMA, la CFMJ ou la Gespa (cf. art. 29, al. 1, LBA en lien avec art. 7, al. 1, let. d, OBCBA).
Lors d'une communication de soupçon ou de l'enregistrement dans goAML, il faut indiquer quelle autorité ou quel organisme au sens de l'art. 12 LBA ou l'art. 43a loi sur la surveillance des marchés financiers du 22 juin 2007[49] surveille l'intermédiaire financier (cf. art. 3, al. 1, let. b, OBCBA).

De même, lorsqu'une entité n'a pas d'autorisation officielle au sens strict et qu'il a été établi officiellement, au cours de la procédure d'autorisation, que son domaine d'activités n'est pas soumis à la LBA, seule une vérification sommaire est effectuée pour déterminer si cette entité a joué le rôle d'intermédiaire financier dans un cas concret. Là aussi, des informations peuvent être échangées avec les autorités de surveillance aux conditions énoncées à l'art. 29, al. 1, LBA.

47 Cf. www.finma.ch/fr/finma-public/etablissements-personnes-et-produits-autorises/; www.finma.ch/fr/autorisation/organisme-d-autoregulation-oar/recherche-de-membres-oar/

48 RS **935.51**

49 RS **956.1**

7. Liens

7.1 Suisse

7.1.1 Bureau de communication en matière de blanchiment d'argent

www.fedpol.admin.ch
Office fédéral de la police (fedpol)

www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei.html
Bureau de communication en matière de blanchiment d'argent (MROS)

www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei/meldung.html
Informations sur goAML

7.1.2 Autorités de surveillance

www.finma.ch/fr/
Autorité fédérale de surveillance des marchés financiers (FINMA)

www.esbk.admin.ch
Commission fédérale des maisons de jeu (CFMJ)

www.gespa.ch
Autorité intercantonale de surveillance des jeux d'argent (Gespa)

7.1.3 Associations et organisations nationales

www.swissbanking.org
Association suisse des banquiers (SBVg)

www.abps.ch
Association de banques privées suisses (ABPS)

www.afbs.ch
Association des banques étrangères en Suisse (ABES)

www.svv.ch
Association suisse d'assurances (ASA)

www.vsv-asg.ch
Association suisse des gestionnaires de fortune (ASG)

www.sfama.ch
Swiss Funds & Asset Management Association (SFAMA)

www.svig.org
Schweizer Verband der Investmentgesellschaften (SVIG)

7.1.4 Organismes d'autorégulation

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

www.arif.ch
Association Romande des Intermédiaires Financiers (ARIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

www.oadfct.ch
Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT)

www.polyreg.ch
PolyReg Association générale d'autorégulation

www.sro-sav-snv.ch
OAR de la Fédération suisse des avocats et de la fédération suisse des notaires (OAR FSA/FSN)

www.leasingverband.ch
Association suisse des sociétés de leasing (ASSL)

www.sro-treuhandsuisse.ch
OAR Union suisse des fiduciaires

www.vqf.ch
Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF)

www.sro-svv.ch
OAR de l'Association suisse d'assurances (OAR-ASA)

7.1.5 Organismes de surveillance

www.aoos.ch
OS de l'association suisse des gérants de fortune (AOOS)

www.fincontrol.ch/
FINcontrol Suisse SA

www.osif.ch/
Organisme de Surveillance des Instituts Financiers (OSIF)

www.so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

www.osfin.ch/fr/
Organisation de Surveillance Financière (OSFIN)

7.1.6 Autres

www.ezv.admin.ch
Administration fédérale des douanes (AFD)

www.snb.ch
Banque nationale suisse (BNS)

www.bundesanwaltschaft.ch/mpc/fr
Ministère public de la Confédération (MPC)

www.seco.admin.ch/seco/fr/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html
Secrétariat d'État à l'économie (SECO) (Sanctions économiques sur la base de la loi sur les embargos)

www.estv.admin.ch
Administration fédérale des contributions (AFC)

www.vbs.admin.ch/fr/ddps/organisation/unites-administratives/service-renseignement.html
Service de renseignement de la Confédération (SRC)

www.bstger.ch
Tribunal pénal fédéral (TPF)

7.2 International

7.2.1 Bureaux de communication étrangers

www.egmontgroup.org/en/membership/list
Liste de tous les membres du groupe Egmont, avec parfois un lien vers leur page d'accueil

7.2.2 Organisations internationales

www.fatf-gafi.org
Groupe d'action financière (GAFI)

www.unodc.org
Office des Nations Unies contre la drogue et le crime (ONUDC)

www.egmontgroup.org
Groupe Egmont

www.cfatf-gafic.org
Caribbean Financial Action Task Force (CFATF)

7.2.3 Autres liens

www.interpol.int
Interpol

www.europol.europa.eu
Europol