Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol
Police judiciaire fédérale PJF
Division Analyse criminelle

National Risk Assessment (NRA):

Escroquerie et hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur en tant qu'infractions préalables au blanchiment d'argent

Rapport du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF)

Janvier 2020

Table des matières

Résumé

La transformation numérique croissante de la société s'accompagne, année après année, d'une progression de la cybercriminalité. Une part importante des infractions pénales commises sur Internet sont des escroqueries. Les fonds ainsi obtenus sont ensuite blanchis, en général par l'intermédiaire d'agents financiers. En décembre 2019 par exemple, plus de 3'800 agents financiers ont pu être identifiés et 228, arrêtés dans le cadre d'une vaste opération internationale de lutte contre le blanchiment d'argent soutenue par Europol[1]. Les escroqueries continuent également à être commises en dehors du cyberespace, et la Suisse n'est pas épargnée. Depuis des années, les escroqueries et leur pendant numérique, à savoir l'utilisation frauduleuse d'un ordinateur, constituent une part importante des soupçons signalés au Bureau de communication en matière de blanchiment d'argent (MROS). L'escroquerie, en particulier, est l'une des infractions préalables les plus fréquemment présumées: entre 2004 et 2014, elle pointait au premier rang en faisant l'objet de presque 40 % des communications de soupçons (utilisation frauduleuse d'un ordinateur: 4 %). Les infractions de corruption occupent désormais la première place de ces communications, mais l'escroquerie et, dans une moindre mesure, l'utilisation frauduleuse d'un ordinateur restent souvent des infractions préalables présumées en lien avec des actes de blanchiment d'argent. Le Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF) a donc décidé d'étudier plus précisément les infractions préalables au blanchiment d'argent que sont l'escroquerie et l'hameçonnage (*phishing*) en vue de l'utilisation frauduleuse d'un ordinateur en Suisse.

Lorsqu'elles aboutissent, l'escroquerie au sens du droit pénal et l'utilisation frauduleuse d'un ordinateur peuvent constituer des infractions préalables au blanchiment d'argent et donc un risque potentiel de blanchiment d'argent, dans la mesure où l'infraction pénale n'est pas considérée comme une infraction d'importance mineure. Les statistiques et les sondages auprès des victimes révèlent certes que ces deux infractions sont largement répandues en Suisse, mais qu'elles restent moins fréquentes que d'autres infractions contre le patrimoine telles que le vol. Pour ce qui est des infractions préalables perpétrées à l'étranger qui sont ensuite suivies d'actes de blanchiment d'argent en Suisse, les informations actuelles sont trop lacunaires pour tirer des conclusions précises. Comme pour les infractions préalables commises en Suisse, le montant moyen des dommages correspondants devrait être relativement faible (moins de 10'000 francs dans la plupart des cas). Enfin, de nombreuses escroqueries se soldent par une simple tentative et ne sont dès lors pas des infractions préalables au blanchiment d'argent. Par conséquent, l'escroquerie et l'utilisation frauduleuse d'un ordinateur ne constitueraient au plus qu'un risque moyen de blanchiment d'argent pour la Suisse.

Très variés, les escroqueries et l'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur se différencient fortement par leur nombre de victimes, leur complexité, le montant du dommage ou leur mode opératoire. La plupart sont réalisables à grande échelle avec une charge de travail relativement faible, mais elles génèrent, par cas, des revenus moyens peu élevés. On peut citer, par exemple, les escroqueries sur les magasins en ligne ou les plateformes immobilières, le montant du dommage par victime s'élevant en général à quelques dizaines ou centaines de francs. D'un autre côté, certains phénomènes d'escroquerie qui aboutissent plus rarement rapportent aux criminels des revenus conséquents, mais ils doivent y consacrer en moyenne davantage de temps (p. ex. prestations d'aide ou ordres de virement trompeurs). Le montant du dommage par cas atteint alors régulièrement plusieurs centaines de milliers de francs. Globalement, il est en moyenne un peu plus élevé pour l'État et les entreprises que pour les particuliers. Dans la plupart des cas, des sommes relativement faibles sont blanchies, en général grâce à des agents financiers. Les actes de blanchiment portant

[1] EUROPOL (2019): 228 arrests and over 3'800 money mules identified in global action against money laundering. Communiqué de presse du 4 décembre 2019, https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering.

sur des montants plus substantiels existent, mais ils sont rares. Ainsi, moins de 2 % des communications pour soupçons d'escroquerie transmises au MROS entre 2009 et 2018 concernaient des montants supérieurs à 10 millions de francs.

Le recours à des agents financiers et à des personnes morales domiciliées à l'étranger ainsi que les nombreuses possibilités d'internationaliser les infractions préalables et le blanchiment d'argent connexe, qui découlent des dernières technologies de l'information et de la communication, constituent les principales vulnérabilités. Les informations sur l'utilisation des cryptoactifs en vue d'un blanchiment d'argent consécutif à une escroquerie sont encore lacunaires, mais ces technologies présentent potentiellement une grande vulnérabilité. De même, dans certaines situations, la complexité d'une escroquerie, le recouvrement des valeurs patrimoniales en temps opportun ou la preuve d'une infraction préalable constituent un défi pour les autorités de poursuite pénale.

Les conséquences des escroqueries en tant qu'infractions préalables au blanchiment d'argent sont difficiles à évaluer, mais un mécanisme efficace de défense et de lutte semble les empêcher d'affecter l'ensemble de la société, du secteur financier ou du secteur tertiaire. Les dommages financiers peuvent certes être considérables pour certaines victimes ou pour l'État; les possibilités de recouvrement des avoirs et les prétentions en dommages-intérêts permettent cependant de les atténuer en partie. La législation relative au blanchiment d'argent peut également avoir un effet préventif en autorisant le blocage de certains paiements douteux.

Jusqu'à présent, l'ampleur et l'impact des actes de blanchiment d'argent résultant d'une escroquerie et de l'utilisation frauduleuse d'un ordinateur ne représentent pas, dans l'ensemble, un risque d'importance systémique pour la Suisse. La menace inhérente aux escroqueries en tant qu'infractions préalables au blanchiment d'argent n'a donc pas fondamentalement changé ces dernières années. L'évolution de ces infractions dans un avenir proche dépend essentiellement de celle de la cybercriminalité. Les informations actuelles sont cependant trop maigres pour pouvoir formuler des prévisions précises. Celles-ci nécessitent d'autres études scientifiques menées par un institut de recherche indépendant (p. ex. universités), et en particulier des sondages auprès des victimes d'escroqueries et d'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur.

1 Introduction

1.1 Contexte du rapport NRA et mandat

Le premier rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse (rapport NRA) a été publié en juin 2015[2]. Il a été rédigé par le Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF). Ce groupe a été créé fin 2013 par le Conseil fédéral et a pour mandat la coordination des mesures de lutte contre le blanchiment et le financement du terrorisme au sein de l'administration fédérale. Dans ce cadre, le GCBF est notamment chargé d'assurer une évaluation permanente des risques avec comme objectif d'identifier les nouvelles menaces de blanchiment d'argent et de financement du terrorisme ainsi que d'identifier d'éventuelles mesures pour pallier ces risques»[3]. En mettant en place le GCBF, la Suisse applique les recommandations 1 et 2 du *Groupe d'action financière* (GAFI), qui exigent une évaluation nationale des risques (*national risk assessment*, NRA), une approche fondée sur les risques ainsi qu'une autorité ou un mécanisme de coordination de la politique nationale de lutte contre le blanchiment d'argent et le financement du terrorisme[4]. Cette analyse des risques implique une identification et une évaluation régulières des risques en matière de blanchiment d'argent et de financement du terrorisme («*identify and assess their ML/TF* [*Money Laundering*/*Terrorist Financing*] *risks on an 'ongoing basis'*»)[5].

Lors de l'élaboration du rapport NRA, des informations issues des communications de soupçons au MROS, notamment, ont été évaluées afin d'apprécier le risque pesant sur la Suisse en matière de blanchiment d'argent. D'après ces communications, l'escroquerie était entre 2004 et 2014 l'infraction préalable présumée la plus fréquente (presque 40 % des communications de soupçons; utilisation frauduleuse d'un ordinateur: 4 %)[6]. Depuis, les infractions de corruption occupent la tête du classement – à l'exception de l'année 2016. Les escroqueries restent toutefois des infractions préalables fréquemment signalées. Le GCBF a donc décidé d'étudier plus précisément les infractions préalables au blanchiment d'argent que sont l'escroquerie et l'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur ainsi que les actes de blanchiment consécutifs en Suisse.

Conformément à ce mandat, le présent rapport d'analyse fournit dans un premier temps une vue d'ensemble des principaux acteurs de la prévention et de la lutte contre les escroqueries. Le chapitre 2 aborde les infractions pénales pertinentes et clarifie les premières questions de délimitation. Le risque qui découle, pour la Suisse, des escroqueries en tant qu'infractions préalables au blanchiment d'argent est analysé au chapitre 3. Le chapitre 4 examine quant à lui les vulnérabilités et les défis. Enfin, l'analyse des conséquences éventuelles et l'évaluation récapitulative des risques figurent au chapitre 5.

1.2 Méthodologie

Le présent rapport s'appuie sur la statistique du MROS relative aux communications de soupçons des dix dernières années (de 2009 à 2018), sur l'évaluation de 69 arrêts des tribunaux

---

[2] GCBF (2015a): rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-juni-2015-f.pdf.

[3] GCBF (2015b): communiqué de presse concernant le rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-57750.html.

[4] Cf. GAFI (2012): normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération. Les recommandations du GAFI. Mises à jour en juin 2019. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Recommandations%20du%20GAFI%202012.pdf.

[5] GAFI (2013): National Money Laundering and Terrorist Financing Risk Assessment, FATF Guidance, février 2013. , p. 6.

[6] GCBF (2015a), référence susmentionnée, p. 36.

et des ministères publics entre 2015 et 2018 qui étaient à la disposition du MROS[7] et sur des sources librement accessibles telles que la statistique policière de la criminalité ou celle des condamnations pénales et la littérature spécialisée. Les décisions de justice ont été choisies principalement en fonction de leur diversité. Les arrêts examinés ne sont toutefois pas représentatifs de la fréquence des formes d'escroquerie respectives. En outre, des entretiens ont été menés avec des représentants du MROS et de la Police judiciaire fédérale (fedpol), de la Prévention Suisse de la Criminalité (PSC), du Ministère public de la Confédération (MPC) et d'un ministère public cantonal.

L'évaluation du risque de blanchiment d'argent est au cœur du présent rapport. Pour apprécier ce risque et celui de financement du terrorisme, le GAFI utilise une notion de risque qui englobe trois facteurs: la menace (*threat*), la vulnérabilité (*vulnerability*) et les conséquences (*consequences*)[8].

Les menaces (*threats*) se définissent comme la probabilité qu'une personne ou un groupe de personnes commette des actes de blanchiment d'argent. L'analyse des menaces (*threat assessment*) identifiera l'importance de la menace, en mesurant à la fois son ampleur (élément quantitatif) et ses caractéristiques (élément qualitatif). À cet effet, il convient de distinguer entre menaces potentielles et réelles. La menace potentielle (ou menace abstraite) est définie par la probabilité qu'au vu de certains éléments structurels et contextuels une menace puisse se réaliser. La *menace réelle* (ou menace concrète) se définit comme l'ensemble des menaces qui se sont effectivement réalisées et qui peuvent, en principe, être mesurées.

Les vulnérabilités (*vulnerabilities*) sont l'ensemble des facteurs (structurels et institutionnels) qui rendent la réalisation d'un crime attractive aux yeux de la personne ou d'un groupe de personnes qui veut blanchir de l'argent. La probabilité qu'un risque se réalise est d'autant plus importante que des vulnérabilités existent. Les *vulnérabilités générales* sont inhérentes aux caractéristiques structurelles du pays et de sa place financière. Les *vulnérabilités spécifiques* sont liées aux pratiques et instruments utilisés dans un secteur d'activités donné. Une dernière catégorie est celle des *vulnérabilités liées au dispositif institutionnel* (régulation et surveillance) de lutte contre le blanchiment d'argent.

On entend par conséquences (*consequences*) l'impact que le blanchiment d'argent peut avoir ou le dommage qu'il peut occasionner.

1.3 Vue d'ensemble de la prévention et de la lutte

En Suisse, plusieurs instances s'occupent de prévenir et de combattre l'escroquerie au sens courant[9]. Les principaux acteurs et leur mandat respectif sont présentés brièvement ci-après.

Centre national de compétences en matière de cybercriminalité (NC3) auprès de fedpol
L'Office fédéral de la police (fedpol) est notamment l'office central suisse en matière de cybercriminalité. Il assume donc des tâches correspondantes, en collaboration avec les cantons et au sein du réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK; cf. ci-après). Par exemple, fedpol fournit aux cantons des prestations de forensique informatique, les soutient dans la coordination et le tri des cas et met à leur disposition des compétences (très) spécialisées et des infrastructures. Créé en 2017 auprès de fedpol, le centre national de compétences en matière de cybercriminalité (NC3) rassemble toutes les

[7] Une décision de non-entrée en matière, 42 ordonnances de classement, deux acquittements, dix ordonnances pénales et quatorze condamnations. Dix procédures étaient gérées par le ministère public de la Confédération, les autres relevant des autorités cantonales de poursuite pénale. Au moins 43 de ces procédures découlaient d'une communication de soupçons auprès du MROS.
[8] GAFI (2013), référence susmentionnée, p. 7 et 8.
[9] L'escroquerie au sens courant va au-delà de l'infraction définie à l'art. 146 du Code pénal (CP). Cf. également le chap. 2 du présent rapport.

compétences relatives à la cybercriminalité des domaines des enquêtes, du soutien aux enquêtes et des tâches des offices centraux de fedpol.

Bureau de communication en matière de blanchiment d'argent (MROS) auprès de fedpol[10]
Le MROS auprès de fedpol joue un rôle de relais et de filtre entre les intermédiaires financiers et les autorités de poursuite pénale. Conformément à la loi sur le blanchiment d'argent, ce service national central reçoit, analyse et, si nécessaire, transmet aux autorités de poursuite pénale les communications de soupçons des intermédiaires financiers relatives au blanchiment d'argent, au financement du terrorisme, aux fonds d'origine criminelle ou aux organisations criminelles.

Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)[11]
La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) est chargée par le Conseil fédéral de la protection des infrastructures d'importance vitale pour la Suisse (infrastructures critiques). Elle a principalement pour mission de détecter précocement et de contrer les dangers ainsi que de soutenir les exploitants de ces infrastructures en cas de crise. Son site Internet s'adresse aussi aux particuliers qui utilisent un ordinateur et Internet, ainsi qu'aux petites et moyennes entreprises en Suisse. Afin de renforcer les activités de la Confédération dans le domaine des cyberrisques, le Conseil fédéral a notamment décidé, le 30 janvier 2019, de créer un Centre pour la cybersécurité en se fondant sur les compétences qui existent déjà entre autres au sein du service bien établi qu'est MELANI. Concernant l'hameçonnage, il est possible de signaler à MELANI des courriels ou sites Web douteux[12].

Prévention Suisse de la Criminalité (PSC)[13]
Sur mandat de la Conférence des directrices et directeurs des départements cantonaux de justice et police, la PSC élabore des campagnes de prévention thématiques, des documents et des projets sur le travail de prévention de la police et met en relation cette dernière et ses partenaires de coopération. La prévention des escroqueries, notamment, joue un rôle important en la matière. De plus, la PSC est chargée de la gestion technique de la prévention générale et policière dans le cadre de la formation et de la formation continue de la police.

Plateforme «Coordination Food Fraud» (COFF)[14]
La plateforme COFF est un groupe de travail interdisciplinaire composé de représentants de l'Office fédéral de l'agriculture (OFAG), de l'Administration fédérale des douanes (AFD), de fedpol, des autorités cantonales compétentes dans le domaine des denrées alimentaires et de l'Office fédéral de la sécurité alimentaire et des affaires vétérinaires (OSAV). Elle est chargée de coordonner la lutte contre la fraude alimentaire. Centre de compétences de la Confédération en matière de sécurité alimentaire, l'OSAV crée notamment les conditions permettant de garantir un niveau élevé de sécurité des denrées alimentaires et de protéger les consommateurs contre la tromperie. Il participe aux contrôles nationaux de produits, en collaboration avec d'autres autorités.

Cyberboard
Créé en 2018, le *Cyberboard* est la plateforme suisse de coordination de la lutte contre la criminalité sur Internet. Les autorités fédérales et cantonales de poursuite pénale ainsi que des acteurs de la prévention y participent.

Réseau de soutien aux enquêtes relatives à la cybercriminalité (NEDIK)
fedpol décharge les cantons en assurant la coordination opérationnelle des affaires complexes (inter)nationales et cantonales en collaboration avec le NEDIK ou en qualité de membre de ce

[10] Cf. https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei.html.
[11] Cf. www.melani.admin.ch.
[12] Cf. www.antiphishing.ch.
[13] Cf. www.skppsc.ch.
[14] Cf. https://www.blv.admin.ch/blv/fr/home/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/nationale-kontrollprogramme.html.

réseau. Créé en 2017 à la demande de la Conférence des commandants des polices cantonales de Suisse (CCPCS), le NEDIK entend produire des résultats destinés à la police suisse en coordonnant des tâches opérationnelles courantes. Il s'agit dans un premier temps d'harmoniser autant que possible la collaboration des différents centres, d'obtenir une vue d'ensemble commune des cas et de développer de nouveaux outils de travail qui apporteront une valeur ajoutée à toutes les forces de police. fedpol agit au sein du NEDIK en tant qu'office central national et centre national de compétences et de coordination (cf. ci-dessus).

Autorités de poursuite pénale
En Suisse, la poursuite pénale d'une escroquerie et de l'utilisation frauduleuse d'un ordinateur relève en premier lieu des autorités cantonales compétentes. Nombre d'entre elles confient le traitement des infractions économiques à des unités spécialisées qui disposent des connaissances techniques correspondantes. Lorsque les infractions pénales ont été commises pour une part prépondérante à l'étranger ou dans plusieurs cantons sans qu'il y ait de prépondérance évidente dans l'un d'entre eux, les autorités fédérales de poursuite pénale en matière de criminalité économique peuvent engager leur propre procédure[15]. En matière de fraude fiscale (TVA, impôt anticipé ou droits de timbre), les procédures pénales sont gérées par l'Administration fédérale des contributions ou, pour ce qui est de la TVA lors de l'importation de marchandises, par l'AFD et sont soumises au droit pénal administratif.

2 L'escroquerie en tant qu'infraction pénale

2.1 L'escroquerie en général et objet de l'étude

Au sens courant, l'escroquerie désigne une tromperie délibérée qui s'accompagne d'un dommage pour la victime et d'un avantage pour son auteur. Cette définition courante va bien au-delà du champ d'application en droit pénal et peut être utilisée pour de nombreuses tromperies. Extrêmement variées, celles-ci ont évolué avec les changements sociaux et techniques. Dans sa classification de l'escroquerie, le chercheur Michael Levi différencie les formes d'escroquerie par exemple en fonction du secteur (public ou privé), du sous-secteur (services financiers, services non financiers, etc.) ainsi que de l'activité de la victime et de l'auteur[16]:

[15] En vertu de l'art. 24, al. 1, du Code de procédure pénale du 5 octobre 2007 (CPP; RS 312.0), le Ministère public de la Confédération est compétent lorsque les actes de blanchiment d'argent ont été commis pour une part prépondérante à l'étranger ou dans plusieurs cantons sans qu'il y ait de prépondérance évidente dans l'un d'entre eux. En cas d'escroquerie au sens de l'art. 146 CP ou d'utilisation frauduleuse d'un ordinateur (art. 147 CP), la compétence fédérale est fondée si, en plus des conditions susmentionnées, aucune autorité cantonale de poursuite pénale n'est saisie de l'affaire ou l'autorité cantonale de poursuite pénale compétente a sollicité la reprise de la procédure par le Ministère public de la Confédération (art. 24, al. 2 CPP).
[16] Michael Levi (2008): *Organized fraud and organizing frauds. Unpacking research on networks and organization*, dans: Criminology and Criminal Justice, 12.2008, p. 391. https://www.researchgate.net/profile/Michael_Levi4/publication/249786379_Organized_fraud_and_organizing_fraudsUnpacking_research_on_networks_and_organization/links/0c960532755df02414000000/Organized-fraud-and-organizing-fraudsUnpacking-research-on-networks-and-organization.pdf.

Tableau 1: Classement des escroqueries selon Michael Levi (2008)

Victime par secteur	*Victime par sous-secteur*	*Exemples d'escroqueries*
Secteur privé	Prestataires de services financiers	Escroquerie aux chèques
		Piratage de produits
		Fausse monnaie
		Utilisation frauduleuse de données
		Abus de confiance
		Délit d'initié
		Escroquerie à l'assurance
		Escroquerie au crédit
		Utilisation frauduleuse de cartes de paiement
		Abus lors de marchés publics
	Prestataires de services non financiers	Escroquerie aux chèques
		Piratage de produits
		Fausse monnaie
		Utilisation frauduleuse de données
		Abus de confiance
		Escroquerie au jeu
		Escroquerie au crédit
		Utilisation frauduleuse de cartes de paiement
		Abus lors de marchés publics
	Particuliers	Escroquerie aux dons
		Fraude à la consommation
		Piratage de produits
		Fausse monnaie
		Escroquerie au placement
		Fraude concernant les rentes
Secteur public	Au niveau national	Escroquerie aux subventions
		Abus de confiance (gestion déloyale)
		Abus lors de marchés publics
		Fraude fiscale
	Au niveau local	Abus de confiance (gestion déloyale)
		Fraude fiscale
		Abus lors de marchés publics
	Au niveau international	Abus lors de marchés publics
		Escroquerie aux subventions de l'Union européenne

Non exhaustive, cette classification concerne non seulement les variantes d'une escroquerie qui peuvent relever de l'infraction pénale énoncée à l'art. 146 CP[17] (p. ex. escroquerie au crédit, aux chèques ou au placement), mais également d'autres infractions pénales (p. ex. fraude

[17] Code pénal suisse du 21 décembre 1937 (RS 311.0).

fiscale [art. 59 LHID[18]; art. 186 LIFD[19]], abus de confiance [art. 138 CP], etc.). De plus, chaque infraction reposant sur une tromperie ne constitue pas forcément une infraction préalable au blanchiment d'argent au sens de l'art. 305bis CP. Les valeurs patrimoniales doivent provenir d'un crime ou d'un délit fiscal qualifié. Par conséquent et à l'exception de ce dernier, les infractions préalables entrant en ligne de compte sont passibles d'une peine privative de liberté de plus de trois ans[20]. En relation avec le présent rapport, il faut en outre qu'il y ait tromperie délibérée, celle-ci visant à engendrer chez autrui une représentation divergente de la réalité[21]. Cette tromperie est un élément fondamental de toute escroquerie. Par ailleurs, les infractions suivantes ont en commun de comporter plusieurs échelons. Il faut donc franchir plusieurs étapes avant d'accomplir avec succès l'infraction respective. Ce faisant, d'autres infractions pénales (p. ex. faux dans les titres) sont parfois commises.

Ce rapport se concentre sur deux infractions pénales: l'escroquerie au sens de l'art. 146 CP et l'utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP. Concernant cette dernière infraction, l'accent est mis sur la variante basée sur l'hameçonnage; d'autres formes telles que le *skimming*[22] ne sont pas considérées. Par souci de simplification, ces deux infractions sont regroupées sous les termes génériques d'escroquerie et d'hameçonnage dans le présent rapport.

2.2 Escroquerie (art. 146 CP)

Quiconque induit astucieusement en erreur une autre personne par des affirmations fallacieuses ou par la dissimulation de faits vrais dans le dessein de se procurer un enrichissement illégitime et amène ainsi la victime à effectuer des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers commet une escroquerie au sens pénal (art. 146 CP), qui est passible d'une peine privative de liberté de cinq ans au plus. Si l'auteur fait métier de l'escroquerie, la peine peut aller jusqu'à dix ans.

L'infraction comprend plusieurs phases ou réussites successives qui doivent se réaliser. Objectivement, certaines conditions doivent déjà être réunies pour qu'une escroquerie au sens de l'art. 146 CP soit considérée comme une infraction pénale. La tromperie peut découler d'une affirmation fallacieuse (orale ou écrite) ou de la dissimulation de faits. De plus, elle doit être astucieuse et induire en erreur ou conforter la victime dans son erreur. S'appuyant sur cette dernière, la personne trompée doit ensuite procéder à un acte de disposition de son patrimoine qui lui cause un dommage ou en occasionne un à un tiers et qui enrichit l'escroc ou un tiers. En outre, le dommage et l'enrichissement doit répondre au principe de l'identité matérielle. En d'autres termes, la perte patrimoniale d'une personne doit correspondre au gain patrimonial d'une autre personne, un lien intrinsèque entre les deux étant nécessaire[23].

L'astuce implique un certain degré de responsabilité individuelle de la part du lésé. D'après la jurisprudence du Tribunal fédéral, le lésé est coresponsable notamment lorsqu'il aurait pu se protéger en faisant preuve d'un minimum de diligence raisonnable ou lorsqu'il n'a pas respecté les précautions les plus élémentaires[24]. Dans de tels cas, l'infraction d'escroquerie n'est pas retenue. En revanche, l'astuce est toujours présente lorsque des manœuvres[25] particulières

---

[18] Loi fédérale du 14 décembre 1990 sur l'harmonisation des impôts directs des cantons et des communes (LHID; RS 642.14).
[19] Loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct (LIFD; RS 642.11).
[20] Art. 10, al. 2, CP.
[21] Stefan Trechsel / Dean Crameri (2012): *Art. 146 Betrug*, dans: Stefan Trechsel / Mark Pieth (éditeur): Schweizerisches Strafgesetzbuch Praxiskommentar, 2^{e} édition, Zurich, 2012, p. 739.
[22] Le *skimming* désigne la manipulation de distributeurs automatiques de billets à l'aide de cartes de compte, de cartes de débit ou de cartes de crédit volées ou copiées illégalement dans le but de retirer de l'argent.
[23] ATF 134 IV 210, consid. 5.3, p. 213.
[24] ATF 126 IV 165, consid. 2, p. 171 et 172.
[25] On parle de manœuvres, par exemple, lorsque des justificatifs ou documents falsifiés sont utilisés pour rendre les allégations crédibles.

sont exécutées ou une construction mensongère[26] est mise en place. Dans certaines circonstances, un simple mensonge peut être réputé astucieux, par exemple lorsque le lésé ne peut pas entreprendre de vérifications ou que celles-ci sont particulièrement difficiles, lorsque l'escroc empêche sciemment toute vérification, lorsque l'on ne peut raisonnablement pas attendre du lésé qu'il fasse des vérifications ou lorsque l'on suppose, en raison d'une relation de confiance, qu'il n'en fera pas. Dès lors, l'infraction est retenue uniquement si les faits fallacieux ou dissimulés n'étaient pas vérifiables par la victime ou ne l'étaient que difficilement. Ce faisant, il faut toujours tenir compte des capacités ou des circonstances particulières qui entravent ou facilitent la vérification par la victime[27].

Sur le plan subjectif, l'intention (un dol éventuel suffit) est requise pour toutes les caractéristiques objectives de l'infraction. L'auteur doit déjà avoir le dessein de s'enrichir au moment de l'erreur. De plus, un lien de motivation doit être manifeste entre l'induction en erreur, l'erreur proprement dite et l'acte de disposition du patrimoine.

2.3 Utilisation frauduleuse d'un ordinateur (art. 147 CP)

L'art. 147 CP punit un enrichissement illégitime découlant d'une utilisation incorrecte, incomplète ou indue de données (ou d'un procédé analogue) qui influe sur un processus électronique ou similaire de traitement ou de transmission de données. Ici aussi, l'exécution d'un transfert d'actifs qui occasionne un dommage constitue une condition.

Il n'y a aucune exigence particulière sur le plan subjectif, hormis l'intention et le dessein de s'enrichir. Il convient de noter que le principe de l'identité matérielle entre le dommage et l'enrichissement est requis, comme dans le cas d'une escroquerie[28].

Contrairement à l'escroquerie visée à l'art. 146 CP, on ne trompe pas ici une personne mais une machine (au sens large). En créant cette infraction, le législateur a comblé une lacune légale résultant du progrès technique. La fraude informatique ne pouvait pas relever de l'art. 146 CP, car le processus correspondant ne trompe pas une personne et une machine ne peut pas succomber à une erreur[29]. Selon le message, la norme «réprime le comportement de celui qui, dans un dessein d'enrichissement illégitime, manipule des données ou des systèmes de traitement de données et provoque ainsi un transfert d'actifs qui ne se serait pas produit si les données ou l'ordinateur avaient été utilisés correctement»[30].

La cyber-infraction a été conçue par analogie aux infractions pénales existantes, l'utilisation frauduleuse d'un ordinateur s'inspirant des éléments constitutifs de l'escroquerie au sens de l'art. 146 CP. L'influence exercée sur le processus de traitement ou de transmission de données correspond plus ou moins à la tromperie astucieuse inhérente à une escroquerie. Elle se traduit par un transfert d'actifs au bénéfice de la mauvaise personne. La façon dont l'auteur obtient les données nécessaires importe peu en la matière[31].

---

[26] Une construction mensongère requiert plusieurs mensonges qui sont coordonnés avec finesse et qui peuvent globalement tromper même une victime critique (ATF 135 IV 76, 81). Plusieurs mensonges simples ne suffisent pas.

[27] ATF 6P.172/2000 et 6S.776/2000 du 14 mai 2001, consid. 8. Ces circonstances peuvent être retenues, par exemple, lorsque la victime a une déficience mentale, est inexpérimentée ou est diminuée en raison de l'âge ou d'une maladie, lorsqu'il existe un rapport de dépendance ou de subordination ou lorsqu'une situation d'urgence restreint la défiance de la victime. En revanche, les connaissances spécialisées particulières ou l'expérience professionnelle de la victime lui sont opposables.

[28] Cf. Gerhard Fiolka (2019): *Art. 147*, dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4e édition, Bâle, 2019, p. 3173.

[29] Cf. Fiolka (2019), op. cit. p. 3162 à 3163,

[30] Conseil fédéral (1991): message du 24 avril 1991 concernant la modification du code pénal suisse et du code pénal militaire (infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (dispositions pénales), FF 1991 II 933, 988.

[31] Cf. Fiolka (2019), référence susmentionnée.

2.4 Autres infractions similaires à une escroquerie

Comme indiqué précédemment, le présent rapport se concentre sur les infractions préalables au blanchiment d'argent que sont l'escroquerie et l'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur. Les autres infractions comportant des éléments d'une tromperie ne sont pas l'objet de ce rapport soit parce qu'elles ne relèvent pas du mandat sous-jacent, soit parce que la plupart d'entre elles ne constituent pas en tant que tels une infraction préalable au blanchiment d'argent ou alors uniquement dans leur forme qualifiée. En outre, d'autres infractions pénales comprenant des éléments d'une tromperie sont liées à des exigences ou à des conditions objectives de punissabilité qui, par exemple, restreignent le cercle des auteurs ou des victimes ou impliquent l'ouverture d'une procédure de faillite (en particulier les infractions boursières, les infractions en matière de faillite et les infractions contre le patrimoine qui prennent la forme de délits). Deux exemples illustrent ci-après les points communs et les différences entre ces infractions et l'escroquerie au sens de l'art. 146 CP.

L'art. 163 CP porte sur la banqueroute frauduleuse et la fraude dans la saisie. L'infraction pénale comporte, pour l'essentiel, un acte de tromperie du débiteur ou d'un tiers concernant les actifs et les passifs disponibles au moment de la faillite. La banqueroute frauduleuse et la fraude dans la saisie ne peuvent cependant être considérées comme des infractions préalables au blanchiment d'argent que si l'auteur est également le débiteur[32]. L'ouverture d'une faillite ou l'émission d'un acte de défaut de biens est une condition objective de la punissabilité. Le dommage concerne exclusivement les créanciers, leurs prétentions étant considérées comme un bien juridique protégé dans la procédure de faillite et de poursuite (contrairement à la fortune en cas d'escroquerie). Lorsqu'il commet cette infraction, l'auteur réalise souvent un faux dans les titres, ce qui peut également se produire lors d'une escroquerie[33]. L'acte de tromperie représente certes un aspect essentiel de l'infraction pénale en cas de banqueroute frauduleuse et de fraude dans la saisie, mais à l'inverse de l'art. 146 CP, il y a une restriction du cercle des auteurs et des lésés, en plus de la condition objective de punissabilité.

Dans le domaine fiscal, l'escroquerie qualifiée en matière de prestations et de contributions ainsi que le délit fiscal qualifié sont considérés comme des infractions préalables au blanchiment d'argent. La fraude à la TVA de type carrousel est assimilée à une escroquerie au sens de l'art. 146 CP (cf. infra). En Suisse, l'escroquerie qualifiée en matière de prestations et de contributions[34] fait office d'infraction préalable au blanchiment d'argent depuis 2009 déjà. Jusqu'à fin 2015, cette infraction se limitait toutefois aux échanges transfrontaliers de marchandises et visait donc la contrebande douanière. À la suite de la mise en œuvre des recommandations révisées du GAFI[35], l'escroquerie qualifiée en matière de contributions a été étendue pour que la disposition s'applique également aux infractions correspondantes commises en Suisse. Depuis le 1er janvier 2016, l'infraction concerne donc aussi l'impôt anticipé, la TVA, les droits de timbre, les livraisons réalisées sur le territoire suisse, la fourniture de prestations de services ainsi que l'impôt sur l'alcool et le tabac perçu sur la fabrication en Suisse[36]. De plus, par analogie à l'escroquerie, elle suppose d'induire astucieusement une personne en erreur ou de la conforter astucieusement dans son erreur.

En 2016, la mise en œuvre des recommandations révisées du GAFI a élevé le délit fiscal qualifié au rang d'infraction préalable au blanchiment d'argent à l'art. 305bis, al. 1bis, CP, à condition qu'il y ait une fraude fiscale[37], c'est-à-dire l'utilisation de titres faux, falsifiés ou inexacts

---

[32] Si un tiers (mais pas le débiteur) est l'auteur, la peine encourue est de trois ans au plus. L'infraction pénale n'est alors pas une infraction préalable au blanchiment d'argent.
[33] Alexander Brunner (2007): *Art. 163*, dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2e édition, Bâle, 2007, p. 785 à 797.
[34] Art. 14, al. 4, de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA; RS 313.0).
[35] Cf. loi fédérale du 12 décembre 2014 sur la mise en œuvre des recommandations du Groupe d'action financière, révisées en 2012 (RO 2015 1389).
[36] Conseil fédéral (2013): message du 13 décembre 2015 concernant la mise en œuvre des recommandations du Groupe d'action financière (GAFI), révisées en 2012, FF 2014 585.
[37] Cf. art. 186 LIFD, 59, al. 1, LHID et art. 305bis, al. 1bis CP.

dans le dessein de tromper l'autorité fiscale, et que les impôts soustraits par période fiscale soient supérieurs à 300'000 francs.

Contrairement à l'escroquerie, la fraude fiscale et l'escroquerie en matière de prestations et de contributions ne constituent une infraction préalable au blanchiment d'argent que dans leur forme qualifiée.

3 Menace liée à l'escroquerie et à l'utilisation frauduleuse d'un ordinateur comme infraction préalable au blanchiment d'argent

3.1 Menace générale

D'après le GAFI, la menace provient d'une personne, d'un groupe de personnes, d'un objet ou d'une activité susceptible d'occasionner des dommages à un État ou à une société, par exemple[38]. Une infraction pénale peut donc représenter une menace: lorsqu'elles aboutissent, une escroquerie au sens du droit pénal et une utilisation frauduleuse d'un ordinateur peuvent constituer une infraction préalable au blanchiment d'argent et donc un risque potentiel de blanchiment, dans la mesure où elles ne sont pas considérées comme d'importance mineure au sens de l'art. 172ter CP. Sont en général d'importance mineure les actes non réalisés par métier qui visent une valeur patrimoniale jusqu'à 300 francs et sont punis d'une amende; ils ne sauraient donc être une infraction préalable au blanchiment d'argent[39]. Les simples tentatives d'escroquerie ne sont pas des infractions préalables au blanchiment d'argent, car il n'y a généralement à ce stade aucun actif à blanchir. Comme pour de nombreuses autres infractions, on peut supposer un nombre élevé d'escroqueries et d'utilisations frauduleuses d'un ordinateur qui n'ont pas été dénoncées (chiffre noir de la criminalité). Concernant l'escroquerie, les raisons de cette criminalité cachée sont multiples: une victime ne la constate pas toujours (contrairement au vol, p. ex.). De plus, certaines personnes renoncent à porter plainte, car elles se sentent honteuses, et les entreprises craignent parfois pour leur réputation. Enfin, les actifs dérobés dans le cadre d'une escroquerie ne sont en général pas assurés (par opposition à de nombreux vols pour lesquels l'assureur peut exiger le dépôt d'une plainte). Les sondages auprès des victimes fournissent des renseignements sur la prévalence des escroqueries. La statistique policière de la criminalité (SPC), la statistique des condamnations pénales (SUS), les communications de soupçons au MROS et les signalements à fedpol en matière de cybercriminalité permettent d'affiner les données sur le type et la fréquence des infractions contre le patrimoine en Suisse. Ces dernières statistiques se limitent cependant aux infractions dont les autorités pénales ont eu connaissance.

3.1.1 Sondages auprès des victimes

Réalisé pour la dernière fois en 2015 sur mandat de la Conférence des Commandants des Polices Cantonales de Suisse (CCPCS), le sondage de Biberstein et al. au sujet des expériences et opinions sur la criminalité en Suisse est l'une des enquêtes les plus vastes menées auprès des victimes dans ce pays[40]. Lors de ce sondage, des questions ont été posées afin notamment de déterminer la prévalence des infractions de type «actes frauduleux en tant que consommateur», «fraude par carte de crédit ou de banque» et «actes de violences sur Internet» (y c. l'hameçonnage). Ces infractions se rapprochent le plus des infractions que sont l'escroquerie et l'utilisation frauduleuse d'un ordinateur. À l'époque, 8,5 % des personnes interrogées déclaraient avoir été victimes d'un acte frauduleux en tant que consommateur au

[38] GAFI (2013), référence susmentionnée, p. 7.
[39] Cf. Philippe Weissenberger (2019): *Art. 172ter*, dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4^{e} édition, Bâle, 2019, p. 3550 à 3563.
[40] Biberstein et al. (2016): sondage au sujet des expériences et opinions sur la criminalité en Suisse. Analyses dans le cadre du sondage national de sécurité 2015.

cours des cinq dernières années. En 2015, cette valeur s'inscrivait à 3,5 % pour les fraudes par carte de crédit ou de banque et à 6,6 % pour les actes de violences sur Internet. En 2011, la prévalence s'établissait à 10,5 % pour les actes frauduleux en tant que consommateur et à 2,7 % pour les fraudes par carte de crédit. Le sondage portait également sur le taux de reportabilité des victimes. Dans ces trois catégories de délit, la part des personnes interrogées ayant déposé plainte s'élevait respectivement à 10,5 % (actes frauduleux en tant que consommateur), à 23 % (fraude par carte de crédit) et à 3,9 % (actes de violences sur Internet)[41].

En 2018, Beaudet-Labrecque et al. ont réalisé une étude sur les abus financiers commis à l'encontre des personnes de 55 ans et plus en Suisse[42]. Plus d'un quart des personnes interrogées (28,3 %) ont indiqué avoir été victimes de diverses tentatives d'escroquerie (ou arnaques) au cours des cinq dernières années (cybercriminalité: 27,8 %). L'arnaque a abouti dans 6,6 % des cas (cybercriminalité: 3,1 %)[43]. Se basant sur cette enquête, les auteurs de l'étude ont extrapolé le nombre de personnes de 55 ans et plus qui avaient été exposées à ces formes d'escroquerie ou à la cybercriminalité dans les cinq années précédentes et celles qui avaient subi une perte financière à cette occasion. Les arnaques les plus fréquentes étaient les tentatives d'hameçonnage (extrapolation: 594'421 personnes concernées de 55 ans et plus), l'escroquerie à l'avance de frais (387'666), notamment l'escroquerie dite d'une «personne en détresse»[44] (234'753), et l'escroquerie au placement (202'448). Les victimes ont subi des dommages financiers principalement à cause de l'escroquerie dite d'une «personne en détresse» (60'304), de fausses annonces sur Internet (47'381), d'échanges de devises (23'691) et d'arnaques aux sentiments (*romance/love scamming*; 15'076)[45]. La perte financière moyenne s'inscrit à 6437 francs pour la cybercriminalité (perte médiane: 400 francs) et à 2'100 francs pour les arnaques (perte médiane: 200 francs)[46].

Lors d'une enquête réalisée en 2017 par PwC, 39 % des entreprises suisses interrogées ont affirmé avoir été victimes d'une escroquerie ou d'une autre infraction économique au cours des deux années précédentes. Le détournement d'actifs (51 %), la cybercriminalité (44 %), les comportements commerciaux abusifs (31 %) et la fraude commise par les consommateurs (23 %) figurent parmi les infractions les plus fréquemment citées par ces entreprises. Concernant la cybercriminalité, l'hameçonnage et l'utilisation de maliciels constituaient les deux techniques les plus utilisées (dans respectivement 42 % et 31 % des cas). Les dommages directs de la criminalité économique s'élèvent, en moyenne, à 9,5 millions de francs[47].

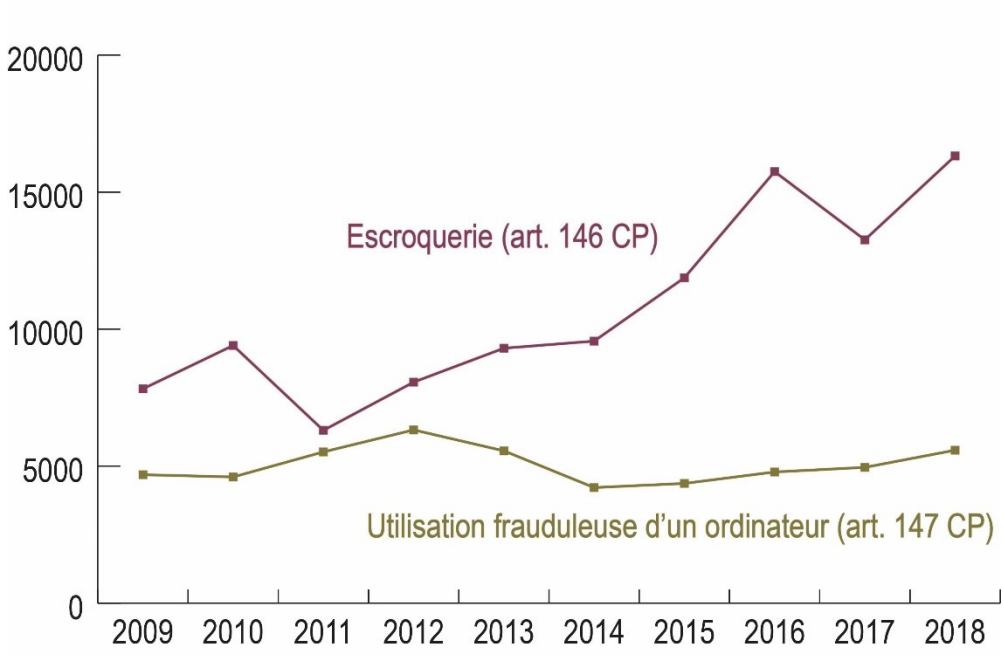
Les sondages auprès des victimes révèlent que les escroqueries touchent, dans l'ensemble, beaucoup de personnes physiques et morales en Suisse et que le nombre de cas non dénoncés est relativement élevé. Ils montrent néanmoins que la plupart des infractions commises auprès des personnes physiques occasionnent des dommages relativement faibles et que ces infractions pénales contre le patrimoine ont parfois une importance mineure et ne peuvent dès lors pas être considérées comme des infractions préalables au blanchiment d'argent. Les montants sont cependant souvent plus élevés pour les personnes morales. Les données issues de ces sondages ne permettent toutefois pas d'évaluer l'évolution temporelle des escroqueries, notamment pour les personnes physiques. De plus, les sondages ne donnent aucune

---

[41] Référence précédente, p. 16 à 21.
[42] Au 31 décembre 2018, on comptait 2,6 millions de personnes de 55 ans et plus parmi la population suisse résidente, soit 31,5 % de la population résidente totale.
[43] Beaudet-Labrecque et al. (2018a): les abus financiers commis à l'encontre des personnes de 55 ans et plus. pp. 15 et 16. https://www.prosenectute.ch/dam/jcr:e0a731a4-ab86-4810-b10c-e4f532374ad4/Finanzieller-Missbrauch-Studienbericht-01.10.2018.pdf.
[44] Cf. exemple d'escroquerie aux dons au point 3.2.3.
[45] Beaudet-Labrecque et al. (2018b): les abus financiers les plus fréquents en Suisse. https://www.prosenectute.ch/dam/jcr:7d5c59ff-5b6b-468c-8666-3a6d21abe729/Finanzieller-Missbrauch-haeufigste-Betrugsformen-in-der-Schweiz-01.10.2018.pdf.
[46] Beaudet-Labrecque et al. (2018a), référence susmentionnée, p. 15 et 16.
[47] PricewaterhouseCoopers (2018): Down but not out: Swiss fraudsters are digitalising and diversifying. Global Economic Crime and Fraud Survey 2018 – Swiss insights, p. 4 à 11. https://www.pwc.ch/en/publications/2018/Global-economic-crime-survey-2018_en_web-double.pdf.

information sur les escroqueries dont les victimes sont à l'étranger, mais dont les actifs à blanchir ont été transférés en Suisse.

3.1.2 Statistique policière de la criminalité (SPC)



Graphique 1: Cas d'escroquerie et d'utilisation frauduleuse d'un ordinateur enregistrés par la police depuis 2009. Source: Office fédéral de la statistique

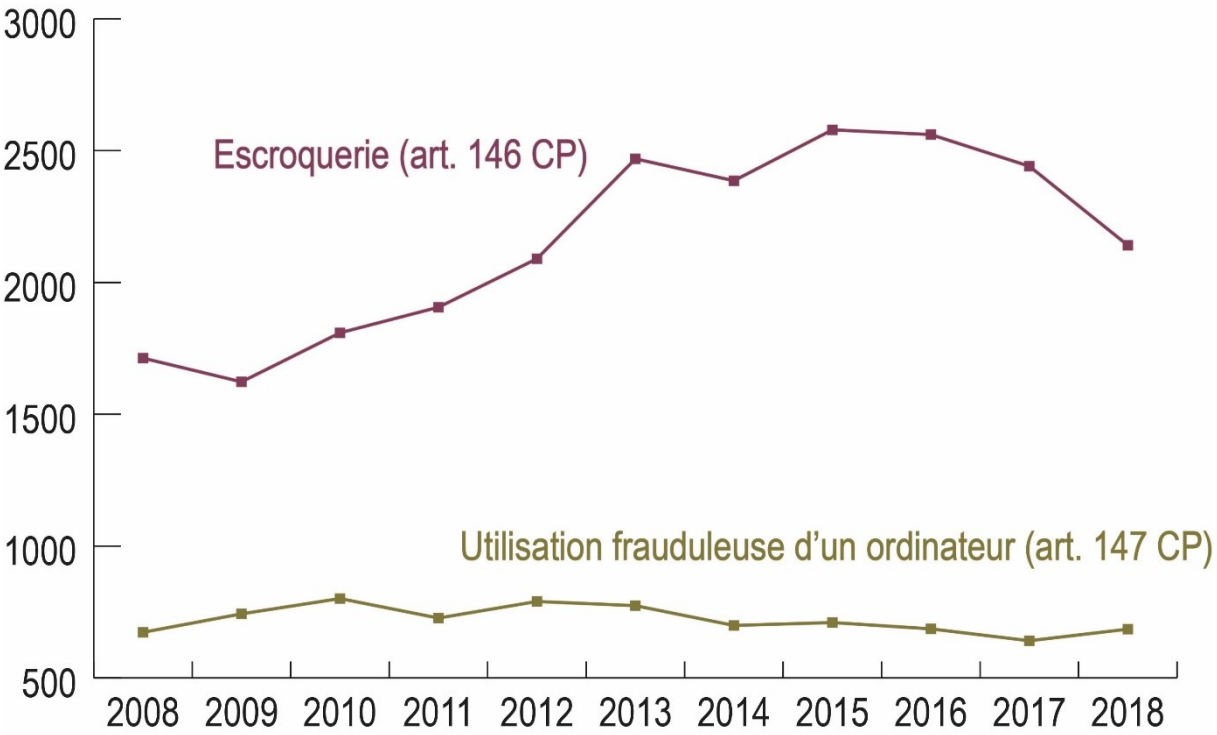
Établie par l'Office fédéral de la statistique (OFS) depuis 2009, la SPC recense toutes les infractions enregistrées par la police. Le nombre d'escroqueries et celui des utilisations frauduleuses d'ordinateurs ont évolué différemment ces dix dernières années. Le volume des escroqueries a plus que doublé depuis 2009, puisque 16'319 infractions pénales ont été déclarées en 2018[48]. En revanche, les utilisations frauduleuses d'ordinateurs sont demeurées relativement stables, malgré une légère progression depuis 2014[49]. On en a compté 5'538 en 2018. Les cantons urbains sont plus fortement touchés, notamment ceux de Bâle-Ville (fréquence 2018 des escroqueries: 5,7 ‰; utilisation frauduleuse d'un ordinateur: 1,6 ‰), de Genève (respectivement 3,2 ‰ et 1,7 ‰) et de Zurich (2,6 ‰ et 0,9 ‰). Les cantons d'Appenzell Rhodes-Intérieures (0,9 ‰ et < 0,2 ‰)[50], d'Appenzell Rhodes-Extérieures et d'Uri (tous deux respectivement 1 ‰ et < 0,2 ‰)[51] ont enregistré le plus faible nombre d'infractions pénales par habitant. En 2018, 85,8 % des escroqueries signalées étaient consommées (utilisation frauduleuse d'un ordinateur: 89,9 %). Ce taux de réussite élevé tient très probablement au fait que la grande majorité des tentatives d'escroquerie et d'utilisation frauduleuse d'un ordinateur ne font pas l'objet d'une plainte. Toutefois, seules les infractions couronnées de succès sont pertinentes pour évaluer le risque de blanchiment d'argent. En 2018, le taux d'élucidation s'établissait à 50,5 % pour les escroqueries (utilisation frauduleuse d'un ordinateur: 31,1 %). Étant donné que seuls les cas résolus la même année par la police peuvent être pris en

[48] Il convient toutefois de noter qu'une seule affaire d'escroquerie peut englober plusieurs infractions pénales et donc influer fortement sur la statistique, comme en 2016 dans le canton d'Argovie (3'920 infractions pénales pour un seul cas).
[49] Le recul observé entre 2012 et 2014 tient probablement à la baisse des cas de *skimming* à la suite de changements techniques et d'une amélioration des mécanismes de contrôle.
[50] Une seule infraction pénale liée à une utilisation frauduleuse d'un ordinateur a été enregistrée dans ce canton en 2018.
[51] Office fédéral de la statistique (2019d): statistique policière de la criminalité (SPC). Rapport annuel 2018 des infractions enregistrées par la police, p. 18. https://www.bfs.admin.ch/bfsstatic/dam/assets/7726192/master.

compte, le taux d'élucidation effectif devrait être un peu plus élevé. Dans l'ensemble, 4'875 personnes se sont rendues coupables d'escroquerie et 1'348, d'une utilisation frauduleuse d'un ordinateur en 2018. Les quatre cinquièmes (81,7 %) faisaient partie de la population suisse résidente (Suisses et étrangers titulaires d'un permis B ou C) dans les cas d'escroquerie. Cette part est légèrement plus faible pour l'utilisation frauduleuse d'un ordinateur (73,2 %). La grande majorité des suspects étaient des hommes (71,4 % pour les escroqueries et 73,2 % pour l'utilisation frauduleuse d'un ordinateur). Globalement, 59,9 % des personnes accusées d'escroquerie avaient entre 20 et 44 ans (utilisation frauduleuse d'un ordinateur: 62,5 %).

Dans l'ensemble, la SPC montre que le nombre d'escroqueries déclarées augmente, tandis que celui des utilisations frauduleuses d'ordinateurs est plutôt stable. Les cantons urbains sont les plus fortement touchés en termes tant absolus que relatifs. La plupart des suspects sont des hommes d'âge moyen qui habitent en Suisse. Les plaintes concernent principalement les infractions qui ont abouti. Globalement, ces deux infractions pénales ne constituaient que 7,6 % des infractions contre le patrimoine enregistrées en Suisse en 2018. La très grande majorité des plaintes déposées dans ce domaine portent sur des vols (2018: 59 %), mais le nombre d'escroqueries non dénoncées pourrait être très élevé.

3.1.3 Statistique des condamnations pénales (SUS)



Graphique 2: Condamnations pour escroquerie et utilisation frauduleuse d'un ordinateur en Suisse depuis 2008. Source: Office fédéral de la statistique

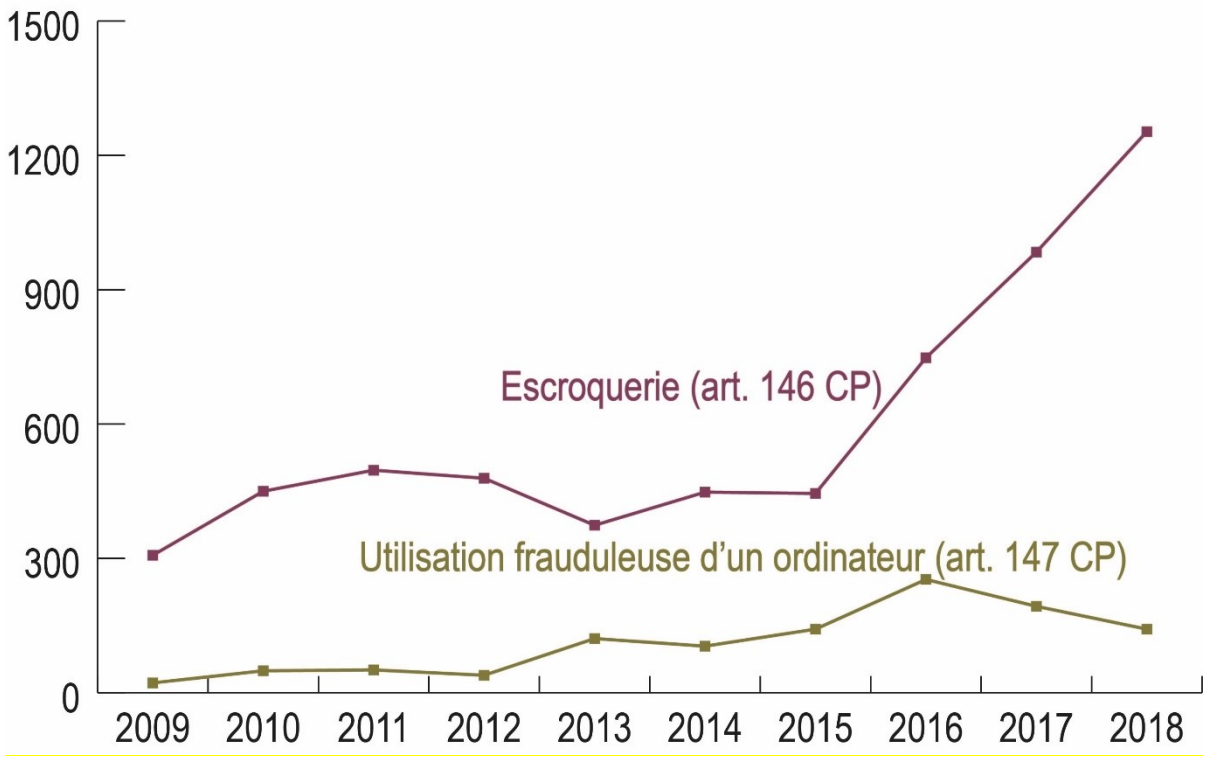
La statistique des condamnations pénales (SUS) existe sous sa forme actuelle depuis 1984. Elle recense l'ensemble des condamnations d'adultes et de mineurs entrées en force et inscrites au casier judiciaire qui ont été prononcées en raison d'un crime ou d'un délit.

Après une hausse entre 2009 et 2015 (malgré un repli en 2014), le nombre de condamnations pour escroquerie diminue. On en dénombrait 2'141 en 2018 (2015: 2'579). Depuis dix ans, les condamnations pour utilisation frauduleuse d'un ordinateur oscillent entre 600 et 800 par an (2018: 685). L'évolution dans la SUS contraste avec l'augmentation observée dans la SPC, en particulier pour l'escroquerie. De plus, les chiffres de la SUS sont sensiblement inférieurs

à ceux de la SPC. Cela tient notamment au fait que la SUS reflète toujours la situation actuelle avec un certain décalage, car les procédures peuvent parfois s'étendre sur plusieurs années jusqu'à l'entrée en force de la condamnation, en particulier pour la criminalité économique. En outre, une infraction ayant fait l'objet d'une plainte ne se solde pas nécessairement par une condamnation. À l'inverse, plusieurs crimes ou délits commis par le même auteur peuvent être regroupés dans un seul jugement pénal. On suppose que des cercles restreints de criminels disposent, grâce aux technologies informatiques les plus récentes, d'un nombre croissant de possibilités d'escroquer beaucoup de victimes. Beaucoup d'escroqueries réalisées avec des outils informatiques, notamment lors d'un hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur, présentent des liens avec l'étranger (cf. entre autres le point 4.1.5). Selon les circonstances, elles peuvent faire l'objet d'une enquête des autorités étrangères de poursuite pénale lorsqu'une procédure est déjà engagée contre les auteurs dans le pays concerné. Par ailleurs, les contraventions relatives aux infractions d'importance mineure contre le patrimoine ne figurent pas dans la statistique. Enfin, une procédure ouverte pour soupçons d'escroquerie peut aboutir à une condamnation pour une autre infraction, par exemple, pour abus de confiance ou faux dans les titres.

En 2018, les condamnations pour escroquerie et utilisation frauduleuse d'un ordinateur constituaient près de 15,7 % des condamnations relatives aux infractions contre le patrimoine. Comme dans la SPC, les vols étaient largement plus fréquents (45,9 %).

3.1.4 Communications de soupçons au MROS



Graphique 3: Communications de soupçons au MROS concernant une escroquerie ou l'utilisation frauduleuse d'un ordinateur comme infraction préalable présumée, depuis 2009. Source: MROS

Les communications de soupçons au MROS donnent des renseignements sur les présomptions d'infractions préalables au blanchiment d'argent. C'est un indicateur adéquat et à jour de ces dernières, car les intermédiaires financiers sont tenus de signaler sans délai leurs soupçons. On notera toutefois que les actes de blanchiment d'argent exécutés sans la participation d'intermédiaires financiers ne figurent pas dans cette statistique. De plus, certains soupçons

se révèlent injustifiés a posteriori. En outre, il n'est pas exclu qu'à ce stade, l'escroquerie serve aussi parfois de terme « fourre-tout » pour classifier certains soupçons. L'évaluation statistique des communications de soupçons réalisées ces dix dernières années (de 2009 à 2018) auprès du MROS est présentée ici.

L'escroquerie (en moyenne 24,4 %) est l'infraction préalable la plus souvent présumée parmi les communications de soupçons qui ont été adressées au MROS ces dix dernières années[52]. L'utilisation frauduleuse d'un ordinateur représentait, quant à elle, environ 5 % des signalements. Le nombre de communications concernant une escroquerie comme infraction préalable présumée a presque triplé entre 2015 et 2018, passant de 445 à 1'253 (+ 182 %). Cette hausse est proportionnellement plus forte que celle qui a été observée pour l'ensemble des communications de soupçons sur la même période (+ 160 %, de 2'367 à 6'144). Entre 2009 et 2018, plus des quatre cinquièmes (84,3 %) des communications de soupçons en lien avec une escroquerie provenaient du secteur bancaire, et en particulier des grandes banques (27,7 % des signalements) ainsi que des banques en mains étrangères (17,6 %). Dans les autres catégories d'intermédiaires financiers, les prestataires du trafic des paiements (7,5 % des communications), les fiduciaires (2 %), les gestionnaires de fortune (1,8 %) et les assurances (1,7 %) jouent un rôle important. Sur la même période, les communications de soupçons portant sur l'utilisation frauduleuse d'un ordinateur émanaient encore davantage du secteur bancaire (93,7 %). Là encore, les grandes banques sont les principaux auteurs des signalements (26,3 %), suivies par les banques cantonales (16,1 %) et les banques Raiffeisen (13,7 %). Dans les autres catégories d'intermédiaires financiers, les prestataires du trafic des paiements (5 %) entrent notamment en ligne de compte. Comme pour les autres infractions préalables, la plupart des communications sont effectuées par le secteur bancaire en raison du nombre relativement élevé de ses clients. De plus, les banques reçoivent des messages SWIFT qui peuvent parfois faire naître des soupçons de blanchiment d'argent.

Plus des quatre cinquièmes des relations d'affaires suspectées se concentrent dans quatre cantons, tant pour l'escroquerie que pour l'utilisation frauduleuse d'un ordinateur: en ce qui concerne les soupçons d'escroquerie, il s'agit de Zurich (39,7 %), de Berne (15,4 %), de Genève (15,2 %) et du Tessin (12,1 %) et, en ce qui concerne les soupçons d'utilisation frauduleuse d'un ordinateur, de Berne (33,1 %), de Zurich (31,2 %), de Saint-Gall (16,4 %) et de Genève (5,9 %). Il s'agit des cantons les plus peuplés et/ou de ceux qui disposent d'une place financière importante. En matière d'escroquerie, le domicile du cocontractant (56,5 % des signalements) et celui de l'ayant droit économique (55 %) se situaient majoritairement en Suisse, les autres principales régions d'origine étant l'Europe de l'Ouest (cocontractant: 18,9 %; ayant droit économique: 24,8 %), l'Amérique centrale et les Caraïbes (respectivement 12,3 % et 1,09 %) ainsi que les États post-soviétiques (2,1 % et 5,3 %). Concernant l'utilisation frauduleuse d'un ordinateur, 90,5 % des cocontractants et 89,7 % des ayants droit économiques étaient domiciliés en Suisse. Loin derrière, l'Europe de l'Ouest était la deuxième principale région d'origine (respectivement 6 % et 6,4 %). La très forte proportion de cocontractants et d'ayants droit économiques habitant en Suisse tient probablement au fait que les criminels y recrutent souvent des agents financiers[53] et que ces relations d'affaires sont ensuite signalées au MROS. En échange d'une commission, ceux-ci mettent leur compte bancaire à disposition et virent ensuite les sommes réceptionnées aux escrocs par courrier ou via des établissements de transfert de fonds, ce qui complique considérablement l'identification des criminels.

Dans plus d'un tiers des cas signalés entre 2016 et 2018 (37,1 %) qui concernent une escroquerie comme infraction préalable présumée, le cocontractant était une personne morale, à savoir une société de domicile (40 % de ces cocontractants) ou une personne morale exerçant

---

[52] La corruption occupe toutefois la première place depuis 2015 – à l'exception de l'année 2016. L'escroquerie est désormais deuxième.

[53] Les agents financiers sont également appelés gestionnaires financiers, intermédiaires financiers, représentants financiers ou *money mules* (cf. également le point 4.1.4).

une activité opérationnelle (60 % restants). Là encore, les personnes morales et les ayants droit économiques étaient surtout domiciliés en Suisse (47 % dans les deux cas). En outre, les personnes morales cocontractantes avaient souvent leur siège en Amérique centrale ou aux Caraïbes (25,4 %) et en Europe de l'Est (17,8 %). Les ayants droit économiques des personnes morales étaient eux aussi essentiellement originaires d'Europe de l'Est (20 %), des États post-soviétiques (10,5 %) ainsi que du Proche et du Moyen-Orient (7,3 %). On suppose que les manœuvres frauduleuses d'envergure, principalement, utilisent des groupes de sociétés complexes pour dissimuler l'origine des fonds acquis de manière illégitime.

Depuis juin 2015, les communications de soupçons précisent également la région de l'infraction préalable. Cette indication est très intéressante, car elle renseigne sur les infractions préalables commises à l'étranger qui utilisent ensuite frauduleusement la place financière suisse pour blanchir l'argent. Les données (de juin 2015 à décembre 2018) révèlent cependant que la Suisse reste le lieu principal de l'infraction préalable: 44 % des escroqueries présumées y ont été réalisées (utilisation frauduleuse d'un ordinateur: 64 %). À l'étranger, les escroqueries ont surtout été exécutées en Europe de l'Ouest (22 %; utilisation frauduleuse d'un ordinateur: 14 %), dans les États post-soviétiques (respectivement 9 % et 0,4 %) et en Amérique du Nord (3 % et 2 %). Toutefois, aucune région n'a pu être attribuée à l'infraction préalable dans 12 % des cas d'escroquerie (utilisation frauduleuse d'un ordinateur: 18 %).

Les intermédiaires financiers ont surtout communiqué des soupçons s'appuyant sur des informations de tiers (escroquerie: 35,9 %; utilisation frauduleuse d'un ordinateur: 84,6 %). Il s'agit fréquemment de réclamations des lésés et de messages SWIFT. Ces derniers expliquent au moins en partie pourquoi la majorité des communications de soupçons proviennent du secteur bancaire. Concernant l'escroquerie, les articles de journaux (26,2 %), les informations des autorités de poursuite pénale (14,7 %) et le propre suivi des transactions (7,8 %) sont également des vecteurs importants des signalements.

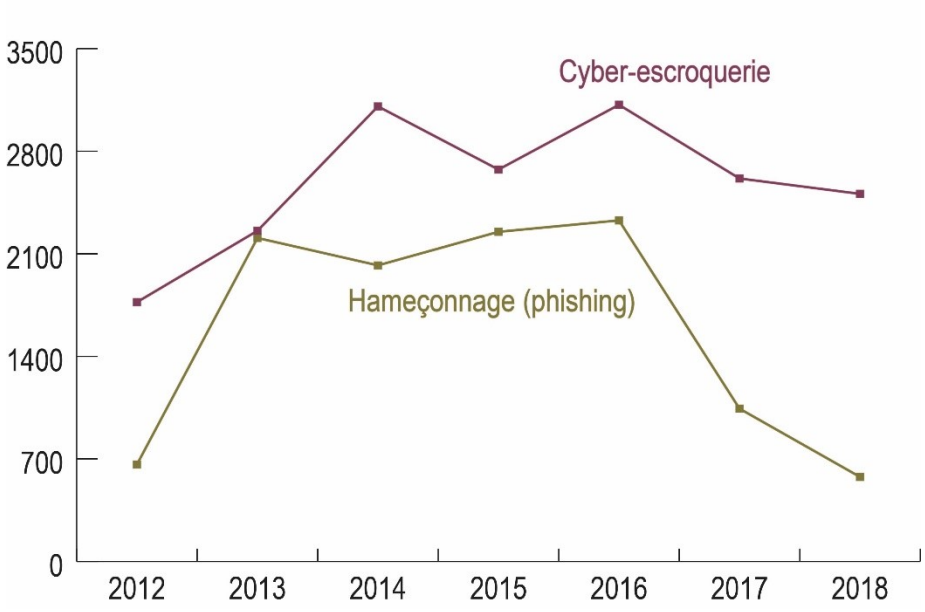
Dans la plupart des communications de soupçons au MROS, les sommes en jeu sont relativement faibles, comme celles qui ressortent des sondages auprès des victimes. Elles étaient inférieures à 1'000 francs dans près de la moitié des cas d'escroquerie (53 %) ou d'utilisation frauduleuse d'un ordinateur (46 %). Globalement, les deux tiers des signalements d'escroquerie (67 %) et les quatre cinquièmes des communications relatives à l'utilisation frauduleuse d'un ordinateur (79 %) portaient sur des dommages de 10'000 francs maximum. Les montants supérieurs à 1 million de francs faisaient l'objet de respectivement 7,7 % et 0,5 % des signalements. Les escroqueries concernent donc plutôt des montants plus élevés, mais cela reste assez rare.

Dans près de la moitié des cas, la communication de ces deux types d'infractions n'a aucune conséquence pénale (signalement non transmis après l'analyse du MROS, non-entrée en matière, suspension ou classement de la procédure). Un jugement a été rendu dans environ 4 % des escroqueries signalées entre 2009 et 2018; l'issue des autres communications est encore en suspens. Le taux de condamnation pour les communications de soupçons d'une utilisation frauduleuse d'un ordinateur est de 26,5 %, soit nettement supérieur à celui des signalements d'escroquerie (issue en suspens fin 2018: 26,5 %). Pour cette dernière infraction, l'agent financier est généralement condamné, mais pas l'auteur principal.

Cette évaluation statistique révèle que les escroqueries présumées sont souvent à l'origine d'une communication au MROS. Dans près de la moitié des cas, les soupçons sont cependant injustifiés ou ne peuvent pas être prouvés ou alors les faits sont prescrits. L'élément subjectif de l'infraction n'est fréquemment pas retenu chez les agents financiers en particulier, ceux-ci faisant l'objet de la majorité des signalements. De plus, il est possible que l'escroquerie soit parfois utilisée comme un état de fait de portée générale lorsque l'infraction préalable n'est pas attribuable précisément. La hausse constatée ces dernières années est conforme aux enseignements tirés de la SPC. Il est probable que les relations d'affaires signalées concernent surtout des cas avec des agents financiers. Cela ressort également du fait que les montants en question sont relativement faibles et que la plupart des cocontractants et des ayants

droit économiques habitent en Suisse. Au moins une partie des escroqueries ont dû être menées à l'aide de montages impliquant des sociétés de domicile à l'étranger pour dissimuler l'origine des fonds. Même si la majorité des infractions préalables sont commises en Suisse, les statistiques du MROS indiquent que l'infraction est souvent réalisée à l'étranger et que les fonds sont ensuite blanchis en Suisse, en particulier pour les cas d'escroquerie.

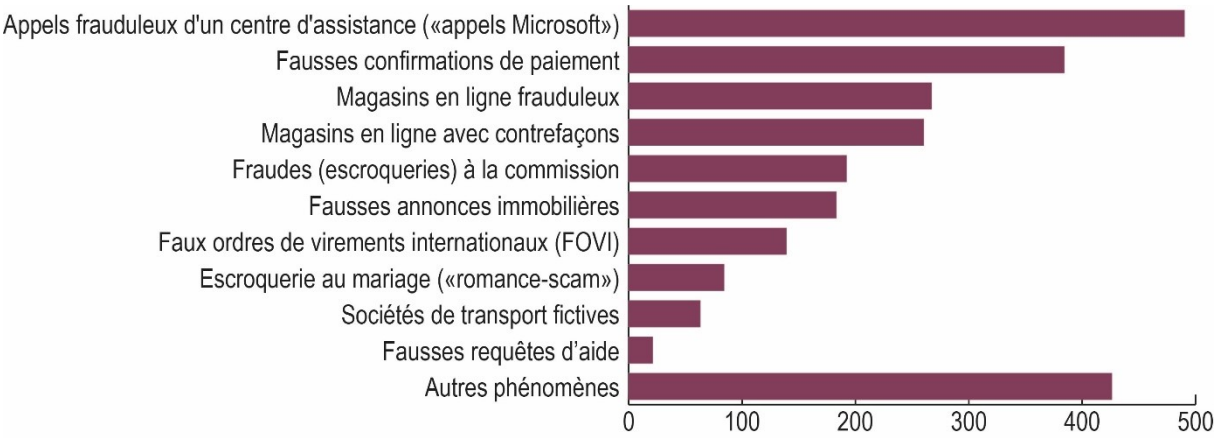
3.1.5 Soupçons de cybercriminalité communiqués à fedpol



Graphique 4: Soupçons de cybercriminalité communiqués à fedpol entre 2012 et 2018

La population transmet à fedpol des soupçons de cybercriminalité (cf. point 1.3) grâce à un formulaire en ligne. La plupart d'entre eux relèvent des dispositions pénales des lois suisses. Leur nombre ne permet toutefois pas de tirer des conclusions pertinentes sur l'ampleur réelle de la cybercriminalité ni sur l'augmentation ou la diminution des contenus illégaux sur Internet. Il ne reflète que la manière dont la population perçoit les contenus et agissements délictueux sur Internet et la volonté de communiquer activement ces soupçons à la police et à d'autres autorités[54]. Depuis quelques années déjà, les annonces les plus fréquentes à fedpol concernent la cyber-escroquerie et l'hameçonnage au sens large. Ces quatre dernières années, ces deux phénomènes ont fait l'objet de plus de la moitié des communications sur la cybercriminalité. fedpol a établi une répartition détaillée des formes d'escroquerie pour l'année 2018.

[54] Office fédéral de la police fedpol (2015): rapport annuel 2014 du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), p. 2. https://www.fedpol.admin.ch/dam/data/fedpol/cybercrime/Berichte/2015-03-26/jb-kobik-f.pdf.



Graphique 5: Soupçons de cybercriminalité communiqués à fedpol en 2018

Cette statistique détaillée met en lumière une vaste gamme de procédés. En 2018, les signalements concernaient en particulier les appels de faux services d'assistance (destinés à enrichir les criminels), les fausses confirmations de paiement et les magasins en ligne frauduleux. On observe à cet égard un nombre croissant de nouveaux modes opératoires. fedpol est informé très rapidement des nouveaux phénomènes et sert d'interlocuteur à ses partenaires.

3.1.6 Évaluation de la menace générale

Les sondages auprès des victimes révèlent que les escroqueries et les utilisations frauduleuses d'ordinateurs sont très répandues en Suisse et que seule une partie d'entre elles fait l'objet d'une plainte. De très nombreux cas ne dépassent cependant pas le stade de la tentative, tandis que d'autres doivent être considérés comme des infractions d'importance mineure contre le patrimoine et ne constituent dès lors pas des infractions préalables au blanchiment d'argent. La plupart du temps, le montant du dommage par victime s'élève à quelques centaines ou milliers de francs; des montants plus élevés sont certes recensés, mais ils sont nettement plus rares. Seuls 20 % des communications de soupçons auprès du MROS qui portent sur une escroquerie en tant qu'infraction préalable concernent des sommes supérieures à 10‘000 francs. Par ailleurs, les escroqueries ne constituent qu'une infime partie des infractions contre le patrimoine en Suisse; leur nombre est nettement inférieur à celui des vols, tant dans la SPC que dans la SUS. De même, les sondages auprès des victimes montrent que le taux de prévalence des vols est plus élevé que celui des escroqueries ayant réussi. Certaines statistiques, en particulier la SPC et les communications au MROS, indiquent une progression des escroqueries en Suisse ces dernières années. Cela découle vraisemblablement d'un transfert partiel des infractions «classiques» contre la propriété vers la cybercriminalité, cette dernière englobant plusieurs types d'escroqueries réalisées grâce à Internet (hameçonnage, escroqueries à l'avance de frais, etc.). Concernant les communications de soupçons au MROS notamment, il se peut aussi que l'augmentation observée résulte d'une meilleure identification des escroqueries par les intermédiaires financiers. Les informations actuelles ne permettent toutefois pas d'étayer cette hypothèse.

Par conséquent, l'escroquerie et l'utilisation frauduleuse d'un ordinateur représentent au plus un risque potentiel moyen de blanchiment d'argent pour la Suisse, en particulier, car, (i) même si elles sont fréquentes, les escroqueries ne le sont de loin pas autant que d'autres infractions contre le patrimoine, (ii) les dommages se montent en général à quelques centaines ou milliers de francs et (iii) seules des escroqueries réussies non assimilées à une infraction d'importance mineure peuvent constituer une infraction préalable au blanchiment d'argent. Eu égard à l'hétérogénéité des escroqueries, la menace éventuelle peut varier d'un phénomène à l'autre, comme cela est précisé dans les sections ci-après.

Le risque concret de blanchiment d'argent ne saurait être chiffré avec précision, car ni la SPC ni la SUS ne permettent d'analyser le blanchiment d'argent en fonction de l'infraction préalable. Ces dix dernières années (de 2009 à 2018), le MROS a reçu 5’985 communications relatives

à une escroquerie en tant qu'infraction préalable présumée. Jusqu'à présent, 255 jugements ont été rendus (utilisation frauduleuse d'un ordinateur: 1'116 communications et 296 jugements). Dans l'ensemble, entre 180 et 450 jugements sont prononcés chaque année en Suisse en matière de blanchiment d'argent, beaucoup portant sur une autre infraction préalable qu'une escroquerie[55]. En termes de volume, les escroqueries représentent globalement un risque concret de blanchiment d'argent plutôt faible, comme le confirment les jugements.

3.2 Menace liée à des phénomènes d'escroquerie spécifiques

Les escroqueries sont variées. Il n'en existe aucune liste exhaustive, car les criminels inventent régulièrement de nouveaux modes opératoires[56]. L'analyse des jugements relatifs aux escroqueries ainsi que de sources publiques et internes à la police a toutefois permis d'identifier certains schémas et phénomènes récurrents qui sont exposés ci-après et évalués en fonction de la menace qu'ils représentent. Ceux-ci sont répartis par catégorie de victimes en se basant sur la classification de Michael Levi (cf. point 2.1). Comme toute classification, il s'agit d'une simplification de la réalité qui vise à proposer une meilleure vue d'ensemble; il en va de même pour le codage en phénomènes. Dans la pratique, plusieurs modes opératoires peuvent être utilisés pour un même cas.

Lorsqu'elle est disponible, la terminologie courante utilisée en Suisse pour le phénomène concerné a été employée. Elle est cependant loin d'être uniforme et se réfère, selon le cas, au but de l'escroquerie (p. ex. escroquerie au crédit), au lésé (p. ex. escroquerie à l'assurance) ou au mode d'exécution (p. ex. hameçonnage). Certains termes sont toutefois déjà fortement ancrés dans le vocabulaire, de sorte qu'une modification entraînerait plutôt une certaine confusion. De nombreuses escroqueries s'appuient sur l'ingénierie sociale (*social engineering*), c'est-à-dire le fait d'influencer et de manipuler une personne de manière ciblée en exploitant, par exemple, sa serviabilité et sa crédulité pour obtenir des données ou l'amener à réaliser certaines opérations. Internet est utilisé à cette fin (*cyber-enabled crimes*).

3.2.1 Phénomènes d'escroquerie visant le secteur public

Les infractions comportant des éléments de tromperie au détriment de l'État relèvent souvent d'états de fait spéciaux qui ne sont pas abordés dans ce rapport (cf. point 2.4). De plus, nombre d'entre elles sont considérées comme des délits ou punies d'une contravention et ne constituent dès lors pas une infraction préalable au blanchiment d'argent (p. ex. obtention illicite de prestations d'une assurance sociale ou de l'aide sociale [art. 148*a* CP] ou fraude fiscale dans sa forme non qualifiée). Des escroqueries au sens de l'art. 146 CP portent cependant régulièrement atteinte au patrimoine de l'État, et des utilisations frauduleuses d'ordinateurs au préjudice du secteur public sont également possibles de manière isolée. Les escroqueries liées aux faillites d'entreprises sont ainsi répertoriées ci-après. Une faillite concerne en général des créanciers, mais les pouvoirs publics font souvent partie des principaux lésés. Il convient également de mentionner d'autres phénomènes d'escroquerie liés à l'État, tels que la fraude à la TVA de type carrousel et les fraudes dans le cadre de marchés publics.

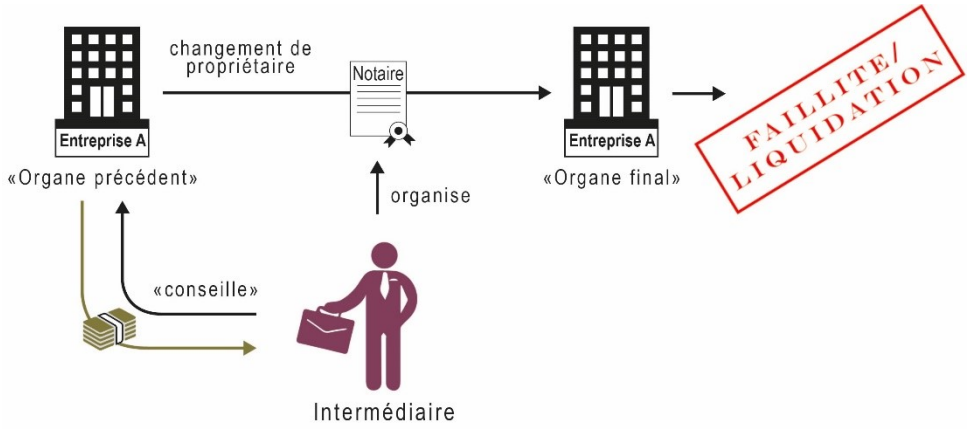
---

[55] D'après les dernières données disponibles pour la période 2008-2012, le trafic de stupéfiants était l'infraction préalable au blanchiment d'argent la plus fréquente (61 % des jugements en matière de blanchiment). L'escroquerie occupait la deuxième position (10 %). Office fédéral de la police fedpol (2014): jugements prononcés en Suisse en matière de blanchiment d'argent. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/geldwaeschereiurteile_okt2014-f.pdf.

[56] fedpol établit et met régulièrement à jour des aide-mémoires sur les phénomènes liés à la cybercriminalité. Ces aide-mémoires contribuent également à identifier les infractions concernées. Cf. Office fédéral de la police fedpol (2020): les différentes formes d'escroquerie (https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/gefahren/betrugsarten.html) et Office fédéral de la police fedpol (2018): dangers liés à Internet (https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/gefahren.html).

a) Escroqueries liées aux faillites d'entreprises

Les infractions en relation avec les faillites d'entreprises concernent généralement la banqueroute frauduleuse[57], la diminution effective de l'actif au préjudice des créanciers[58] et la gestion fautive[59]. Selon le cas, on peut également être en présence d'une escroquerie au sens de l'art. 146 CP, comme pour les «abonnés aux faillites». Dans ce mode opératoire, des petites entreprises qui ne peuvent plus honorer leurs dettes (organe précédent) s'adressent à des intermédiaires notoirement connus qui reprennent les sociétés et effectuent les formalités requises en échange d'honoraires de conseil. Ces intermédiaires garantissent aux organes précédents qu'ils peuvent ainsi se soustraire à leur responsabilité personnelle et remplacer la société endettée par une nouvelle. Ils les incitent à commander d'autres biens sur facture ou à conclure des contrats de leasing pour des véhicules qui seront ensuite revendus à l'étranger. Dès que les entreprises surendettées ont été suffisamment exploitées, elles sont reprises par un organe final. Mis en place par les intermédiaires, celui-ci se compose en général de personnes sans fortune ni activité lucrative qui n'ont aucune expérience dans la gestion d'une entreprise. La principale tâche des organes finaux consiste à se distancier autant que possible des organes précédents, tant sur le plan temporel et spatial qu'en termes de contenu, pour diminuer le risque que ces organes précédents soient tenus d'acquitter leurs obligations auprès des créanciers, des offices des faillites ou des autorités de poursuite pénale[60]. Pour ce faire, les organes finaux sont indemnisés par les intermédiaires. Après un certain temps, les sociétés sont liquidées ou font l'objet d'une ouverture de faillite. Même si l'on remarque à ce moment-là que l'organe final est aussi en relation avec d'autres sociétés mises en faillite, l'objectif est atteint: la société est radiée d'office en raison du manque d'actifs et les coûts sont amortis. Cela occasionne un dommage non seulement aux créanciers privés, mais également et surtout aux pouvoirs publics[61]. La plupart des organes précédents et finaux peuvent être poursuivis pour différentes infractions liées à la faillite[62] et pour escroquerie[63], tandis qu'une enquête pour entrave à l'action pénale, escroquerie et instigation à commettre des délits liés à la faillite est généralement ouverte contre les intermédiaires.



Graphique 6: Exemple de banqueroute frauduleuse

[57] Art. 163 CP.
[58] Art. 164 CP.
[59] Art. 165 CP.
[60] Senad Sakic (2015): Gewerbsmässige Firmenbestattung. Thèse de master au Competence Center Forensik und Wirtschaftskriminalität (centre de compétence en matière de forensique et de criminalité économique). Haute école de Lucerne. 2015, p. 6.
[61] Référence susmentionnée, p. 15.
[62] Banqueroute frauduleuse et fraude dans la saisie (art. 163 CP), diminution effective de l'actif au préjudice des créanciers (art. 164 CP), gestion fautive (art. 165 CP), violation de l'obligation de tenir une comptabilité (art. 166 CP).
[63] Fraude à la commande et au leasing (art. 146 CP).

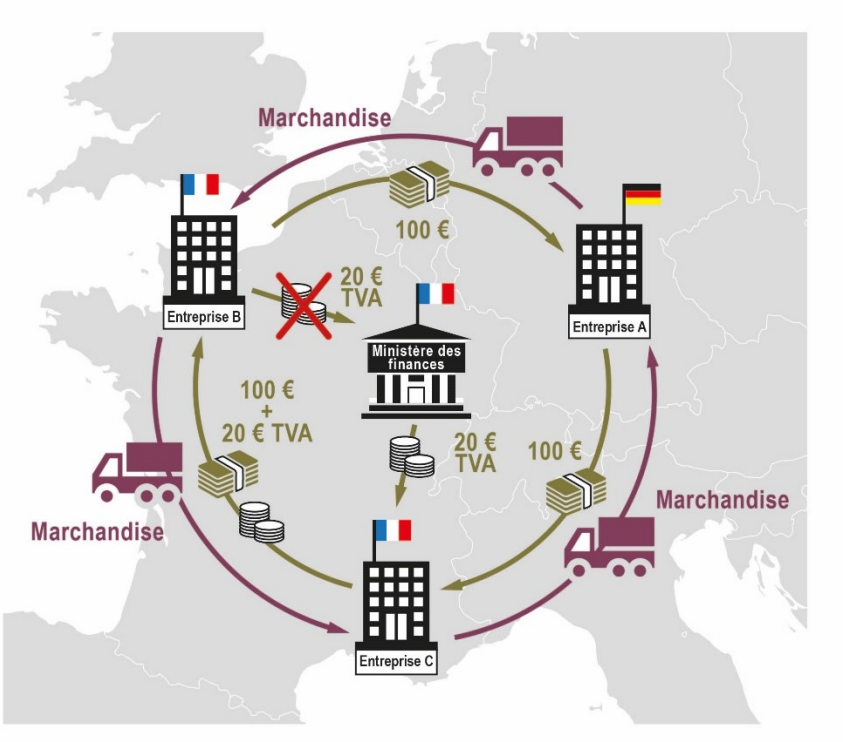
Le nombre d'ouvertures de procédures de faillites à l'encontre de sociétés et de personnes augmente en Suisse depuis l'an 2000, passant de 8'712 à 15'291 en 2018. Les dommages financiers résultant de procédures de liquidations ordinaires et sommaires s'élevaient à environ 2 milliards de francs en 2018[64]. La part résultant d'actes frauduleux ne peut être estimée que sommairement. En 2016, les autorités zurichoises considéraient que les faillites abusives occasionnaient un préjudice annuel de plus de 200 millions de francs pour le canton[65]. Extrapolé à l'échelle nationale, le dommage annuel dépasserait 1 milliard de francs.

Les chiffres de la SPC et de la SUS sont bien plus modestes, mais indiquent que ce phénomène tend à augmenter. Par exemple, le nombre de jugements pour gestion fautive a plus que quintuplé entre 2008 et 2018 pour s'établir à 237 (contre 41 auparavant). L'évolution de la banqueroute frauduleuse n'est pas aussi marquée, mais elle va dans la même direction (240 jugements en 2018; 115 en 2008). Le volume des cas non identifiés est probablement considérable. Les informations disponibles ne permettent pas d'évaluer la part des montants qui ont ensuite été blanchis. Comme indiqué précédemment, les infractions liées aux procédures de faillite ne constituent pas toutes une infraction préalable au blanchiment.

b) Fraude à la TVA de type carrousel

Ce type de fraude vise principalement à permettre à une entreprise de déduire l'impôt préalable sans que la TVA ne soit jamais versée. Le mode opératoire est exposé ici de manière simplifiée (cf. graphique 7): l'entreprise B, qui a son siège dans un pays européen (France), prétend acheter des biens ou des services d'une valeur de 100 euros à l'entreprise A, domiciliée dans un autre pays européen (Allemagne). Cette opération étant une livraison intracommunautaire, elle est exonérée d'impôt d'après la législation européenne sur la TVA. L'entreprise B livre ensuite ces biens ou services généralement fictifs à la société C, dont le siège se trouve dans le même pays que B. Ce deuxième niveau du carrousel n'étant plus exempté d'impôt, B facture à C le prix des biens plus la TVA échue (soit 100 euros plus 20 euros de TVA). Comme l'ensemble du négoce est purement fictif, il n'y a en général aucun flux financier. L'entreprise B devrait à présent transmettre la TVA au ministère des finances, mais elle n'honore pas cet engagement. Dans ce système, elle est considérée comme un opérateur défaillant (*missing trader*), car elle disparaît dès que le carrousel est découvert. Il s'agit la plupart du temps de sociétés de domicile dirigées par des hommes de paille. La société C revend ensuite les biens à A. On est dès lors de nouveau en présence d'une livraison intracommunautaire qui n'a aucune incidence fiscale pour C ou pour A. La société C peut cependant faire valoir la TVA versée auparavant à B comme déduction de l'impôt préalable, de sorte que le ministère des finances lui rembourse les 20 euros. Globalement, les escrocs se sont ainsi fait «rembourser» la TVA sans ne jamais l'avoir acquittée. À présent, l'entreprise A revend de nouveau les biens à B et le carrousel recommence à tourner. Dans la plupart des cas, d'autres entreprises intermédiaires opèrent principalement entre B et C pour masquer la complicité des deux entreprises et compliquer les enquêtes. Ces sociétés tampons (*buffer*) n'ont souvent pas conscience d'être utilisées pour une fraude de type carrousel.

[64] Cf. Office fédéral de la statistique (2019c): nouvelle augmentation du nombre d'ouvertures de faillites. Version du 11 avril 2019. https://www.bfs.admin.ch/bfsstatic/dam/assets/7966849/master.
[65] RTS (2017): véritable «industrie» de la faillite abusive dans le canton de Zurich. 28 avril 2017. https://www.rts.ch/info/suisse/8577464-veritable-industrie-de-la-faillite-abusive-dans-le-canton-de-zurich.html.



Graphique 7: Représentation schématique d'une fraude à la TVA de type carrousel

D'après une décision du Tribunal fédéral[66], une fraude de type carrousel doit être considérée en Suisse comme une escroquerie au sens de l'art. 146 CP et non, par exemple, comme une escroquerie en matière de contributions. C'est donc depuis longtemps une infraction préalable au blanchiment d'argent. Les auteurs sont surtout des bandes européennes bien organisées, qui se composent pour la plupart d'escrocs récidivistes. À la suite de l'extension de l'UE, un nombre croissant de commanditaires d'Europe de l'Est ont été démasqués dans des fraudes à la TVA de type carrousel.

Il n'existe aucun chiffre fiable sur l'ampleur de ces fraudes en Suisse. Compte tenu du faible taux de TVA par rapport à la moyenne européenne, les autorités fiscales helvétiques ne sont que très rarement lésées. Il se peut toutefois qu'une entreprise tampon soit domiciliée en Suisse. Ce type de fraude illustre parfaitement les crimes pour lesquels l'infraction préalable se déroule à l'étranger et la place financière suisse est ensuite utilisée pour blanchir de l'argent.

c) *Fraude aux marchés publics*

Lors d'une fraude aux marchés publics, un mandat public est adjugé à une personne privée sur la base d'une tromperie astucieuse. L'escroquerie entre principalement en considération lorsque le comportement punissable est imputable au soumissionnaire[67]. Toutefois, un employé de l'administration peut lui aussi se rendre coupable d'escroquerie, par exemple s'il trompe son supérieur hiérarchique sur la légalité du mandat à approuver (cf. exemple). La question de savoir si un cartel de soumission peut également constituer une escroquerie au sens de l'art. 146 CP[68] n'a pas encore été tranchée.

---

[66] ATF 1A.189/2001 du 22 février 2002.

[67] Peter Galli et al. (2013): Praxis des öffentlichen Beschaffungsrechts. Eine systematische Darstellung der Rechtsprechung des Bundes und der Kantone. 3e édition. Zurich, 2013, p. 551.

[68] Cf. Jürg-Beat Ackermann (2019): Das Submissionskartell – Sicht des Strafrechts. Lucerne, 18 février 2019. https://www.unilu.ch/fileadmin/fakultaeten/rf/diebold/Tagung_Submissionskartell/Ackermann_Submissionskartell_Strafrecht.pdf; Galli et al., référence susmentionnée, p. 551 et 552.

Les abus lors de marchés publics de la Confédération, des cantons et des communes sont probablement bien plus répandus que ne le laisse présager le nombre relativement faible de procédures pénales en la matière. À l'étranger aussi, les irrégularités répréhensibles ne sont pas rares lors des acquisitions de l'État. Ces faits relèvent souvent des dispositions pénales régissant les devoirs de fonction et les obligations professionnelles ou du droit pénal sur la corruption. Les escroqueries au sens de l'art. 146 CP sont néanmoins récurrentes, même si les constatations lacunaires ne permettent pas de les estimer précisément.

Exemple de fraude aux marchés publics

A travaillait pendant des années comme chef de projet dans une entreprise publique. Entre 2002 et 2014, il a accordé de manière illicite à trois entreprises des mandats de gré à gré d'une valeur totale supérieure à 11 millions de francs. La majeure partie des prestations facturées n'ont pas été fournies ou ne l'ont été que partiellement. A rédigeait lui-même de nombreuses offres pour des mandats qu'il adjugeait ensuite. Il devait également vérifier les factures émises pour ces soi-disant prestations réalisées, puis les transmettait à son supérieur hiérarchique pour validation. A utilisait les rapports de confiance avec ce dernier, tout en sachant que son supérieur n'était pas en mesure de vérifier l'exactitude matérielle des factures. Le produit du crime est estimé à 600'000 francs. A en a dépensé la majeure partie pour son train de vie et celui de sa famille, pour aller au restaurant et partir en vacances. En juin 2018, le Tribunal pénal fédéral a condamné A à une peine privative de liberté de 36 mois assortie d'un sursis partiel et à une peine pécuniaire de 150 jours-amende avec sursis pour escroquerie par métier, blanchiment d'argent simple, gestion déloyale des intérêts publics, corruption passive et acceptation d'un avantage.

3.2.2 Phénomènes d'escroquerie visant les entreprises

Les entreprises sont des cibles intéressantes pour les escrocs, car ils peuvent y subtiliser des sommes potentiellement élevées. Véritable épine dorsale de l'économie suisse, les petites et moyennes entreprises (PME) sont particulièrement menacées, car elles ne disposent pas toujours des ressources et du savoir-faire nécessaires pour se protéger efficacement contre les manœuvres frauduleuses. Les grandes entreprises peuvent également être victimes d'une escroquerie. Les faux ordres de virements internationaux, l'hameçonnage ainsi que les escroqueries au crédit ou à l'assurance sont des phénomènes fréquents. Les escroqueries liées aux faillites, qui lèsent souvent des entreprises, ont déjà été évoquées plus haut.

*a) Hameçonnage (*phishing*)*

Composé des termes anglais *password* (mot de passe), *harvesting* (moisson) et *fishing* (pêche), le mot *phishing* désigne un processus qui vise à soutirer de façon frauduleuse des données confidentielles à un utilisateur en recourant à la tromperie. Pour ce faire, les criminels envoient, par exemple, des courriels dans lesquels ils invitent la victime à mettre à jour ses données personnelles relatives à ses comptes e-mail, ses cartes de crédit ou son système e-banking. Les courriels d'hameçonnage sont souvent envoyés grâce à des réseaux d'ordinateurs compromis (*botnets*). La plupart des sites d'hameçonnage sont hébergés à l'étranger et peuvent se trouver sur les serveurs piratés de tiers. Les données volées peuvent être revendues et réutilisées par d'autres criminels. En général, l'envoi de courriels d'hameçonnage n'est pas punissable. En revanche, selon la configuration des pages Internet ou des courriels falsifiés, l'infraction de faux dans les titres peut être retenue[69]. Si les criminels se servent des données reçues pour transférer des actifs au détriment du lésé, il y a alors utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP. Au niveau de l'État ou des entreprises, l'hameçonnage peut aussi être destiné à de l'espionnage (art. 272 à 274 CP). Comme les banques

[69] Cf. ATF 116 IV 343.

ont régulièrement amélioré leurs mesures de sécurité ces dernières années, les groupes criminels utilisent depuis fin 2006 un nombre croissant de maliciels (*malwares*) pour modifier les paramètres DNS et rediriger ainsi la victime, à son insu, vers un site Web falsifié où elle saisira des informations confidentielles (*pharming*). S'ils parviennent à transférer illégalement des fonds, leurs actes relèvent ici aussi de l'utilisation frauduleuse d'un ordinateur[70]. Pour masquer les traces des fonds obtenus frauduleusement, la plupart des escrocs font appel à des agents financiers qui, en échange d'une commission, mettent leur compte à disposition pour des paiements délictueux. Dès que l'argent est crédité sur le compte d'un agent financier, celui-ci a l'ordre de retirer la somme en espèces et de la virer à un destinataire inconnu par courrier ou via un établissement de transfert de fonds.

L'ampleur exacte de l'hameçonnage est difficile à évaluer, car de nombreuses tentatives sont automatiquement déjouées par les filtres anti-spams et d'autres mécanismes de protection. Selon une enquête sur la criminalité économique menée en 2017 par PwC, le *phishing* était la technique de cybercriminalité la plus souvent utilisée contre les entreprises[71]. Les particuliers sont eux aussi fortement touchés par ce phénomène. En 2018, des extrapolations réalisées lors de l'étude de Beaudet-Labrecque et al. indiquaient que plus d'un demi-million de personnes de 55 ans et plus avaient été confrontées à une tentative d'hameçonnage en Suisse au cours de cinq dernières années (soit une prévalence d'environ 20 %)[72]. Dans les générations plus jeunes, presque chaque personne a probablement déjà été concernée au moins une fois par une tentative de *phishing*. Les 577 communications de soupçons d'hameçonnage transmises sur Internet à fedpol en 2018 ne devraient donc refléter qu'une infime partie de la situation actuelle. Lorsqu'une tentative aboutit, il ne s'agit que d'un acte préalable à un éventuel blanchiment d'argent, car il n'y a encore à ce stade aucun dommage financier.

b) *Faux ordres de virements internationaux (FOVI)*

Ce mode opératoire initialement connu sous le nom d'arnaque au président a donné naissance à plusieurs variantes qui, selon le pays ou l'autorité, sont notamment appelées escroquerie aux faux ordres de virements internationaux, ingénierie sociale (*social engineering*) ou *Business E-mail Compromise Fraud* (BEC)[73]. Les variantes suivantes sont fréquentes:

- Lors d'une *arnaque au président* (au sens strict), les auteurs se font passer pour le directeur ou le responsable financier de l'entreprise contactée. Ils essaient de manière très astucieuse d'inciter les collaborateurs à exécuter un ou plusieurs paiements bancaires en leur faveur. Parfois, les criminels tentent de pirater les comptes e-mail des collaborateurs ou utilisent des adresses e-mail très ressemblantes pour ensuite envoyer des ordres de paiement aux services financiers.
- Dans une *arnaque au faux spécialiste bancaire*, les auteurs visent également des entreprises privées. Ils se font passer au téléphone pour des employés d'une banque et parviennent, grâce à différentes astuces, à accéder à une session e-banking du lésé. Ils exécutent ensuite plusieurs virements en leur faveur. Parfois, ils se présentent comme des partenaires commerciaux (p. ex. avocat, agent immobilier, fournisseur, etc.) et indiquent aux collaborateurs de l'entreprise que les paiements devront être effectués à l'avenir sur un autre compte, contrôlé par les criminels.
- Lors d'une *arnaque au faux agent immobilier*, les auteurs essaient grâce à différentes techniques de modifier les ordres de paiement existants d'une gérance immobilière ou

[70] Office fédéral de la police fedpol (2011b): Agents financiers: le blanchiment d'argent comme activité accessoire lucrative (interne), p. 2.
[71] PricewaterhouseCoopers PwC (2018), référence susmentionnée, p. 10.
[72] Beaudet-Labrecque et al. (2018b), référence susmentionnée.
[73] Cf. Egmont Group of Financial Intelligence Units (2019): *Business Email Compromise Fraud*, dans: Egmont Group Bulletin, p. 3 et 4. https://www.egmontgroup.org/sites/default/files/filedepot/external/20190708_EGMONT%20GROUP%20BEC%20BULLETIN-final.pdf.

d'un agent immobilier. Ils se font passer pour ce dernier ou pour une personne concernée par la transaction et demandent à la victime de transférer l'argent sur un compte qu'ils contrôlent.

Pour être crédibles, ces escroqueries nécessitent une préparation minutieuse qui dure parfois des mois. Les escrocs rassemblent au préalable toutes les informations disponibles sur l'entreprise, son organigramme, ses modalités de paiement, ses relations bancaires, ses secteurs d'activité, ses projets en cours, ses partenariats, etc., et n'hésitent pas à pirater les comptes e-mail des employés. Par téléphone ou par courriel, ils demandent au collaborateur ciblé du service financier d'exécuter sans délai un paiement important, par exemple dans le cadre de l'acquisition encore extrêmement confidentielle d'une autre entreprise. Il n'est pas rare qu'ils contactent préalablement la banque pour annoncer un changement de numéro de téléphone. Si l'employé de banque responsable a des doutes sur la légitimité du virement et souhaite la vérifier, l'escroc sera à l'autre bout du fil et lui confirmera le virement. Parfois, les criminels prennent directement contact avec le conseiller à la clientèle ou la fiduciaire et se présentent comme le directeur de l'entreprise. Pour ce faire, ils utilisent le logo de cette dernière et une adresse e-mail très similaire à celle du directeur. En général, les criminels opèrent depuis l'étranger, et typiquement du Proche-Orient, où les actifs atterrissent régulièrement après un fréquent détour par un pays asiatique. Ce type d'escroquerie concerne aussi bien les PME que les grandes entreprises de tous les secteurs économiques.

Il n'existe aucun chiffre sur l'ampleur totale des faux ordres de virements internationaux en Suisse. Entre 2015 et 2018, 3,8 % des communications de soupçons relatifs à la cybercriminalité réalisées auprès de fedpol concernaient ce phénomène. Pendant cette période, le nombre de déclarations a oscillé entre 95 (2015) et 210 (2017). Pour ce qui est de l'arnaque au président, fedpol a connaissance d'au moins 238 cas qui ont eu lieu entre 2010 et 2017, dont 59 ont été couronnés de succès pour les criminels. Le total des dommages directs s'élevait à plus de 34 millions de francs. Le nombre d'arnaques au président dénoncées tend à reculer non seulement en Suisse, mais également dans plusieurs autres pays, les criminels semblant désormais privilégier d'autres variantes de cette escroquerie.

Les faux ordres de virement devraient être beaucoup plus rares que l'escroquerie à l'avance de frais, par exemple, dont les cas réussis se compteraient par milliers chaque année en Suisse. Les dommages par escroquerie consommée atteignent fréquemment plusieurs centaines de milliers de francs. Dans les cas les plus graves, l'entreprise concernée peut faire faillite. Les transferts de fonds internationaux étant exécutés la plupart du temps vers des États souvent peu coopératifs, un grand nombre d'escroqueries consommées devraient être suivies d'actes de blanchiment d'argent.

c) Escroquerie au crédit

Lors d'une escroquerie au crédit, les criminels essaient d'obtenir un crédit grâce à des informations mensongères sur leurs revenus, leur solvabilité, le but du paiement ou d'autres critères. Ils n'ont pas l'intention de rembourser ce crédit. Dans la plupart des cas, ils utilisent également des documents falsifiés pour demander le crédit. Ce comportement relève de l'escroquerie, la Suisse n'ayant pas d'infraction spécifique pour l'escroquerie au crédit. Par le passé, tant des personnes individuelles que des bandes organisées ont été condamnées pour escroquerie selon ce mode opératoire. Souvent, les criminels ont également été reconnus coupables de blanchiment d'argent, car ils avaient retiré en espèces, transféré ou dépensé le montant des crédits obtenus frauduleusement.

fedpol n'a pas de chiffres fiables sur l'ampleur de ce phénomène. Il devrait y avoir quelques milliers d'escroqueries au crédit chaque année. Il est probable que les criminels ne conservent pas ce butin uniquement sur leurs propres comptes; on peut donc supposer un blanchiment d'argent dans la plupart des cas (contre-exemple: cf. encadré ci-après).

Exemple d'escroquerie au crédit

En 2015, deux personnes originaires d'un pays d'Europe du Sud-Est ont été condamnées dans le canton d'Argovie pour escroquerie par métier et faux dans les titres. Il s'agissait d'un grand nombre d'escroqueries comprenant au total près de 270 infractions dénoncées dont le montant global avoisinait 3,5 millions de francs. L'affaire fut révélée à la suite d'une annonce de blanchiment d'argent effectuée par la banque concernée. En plus des criminels dans le canton d'Argovie, une autre cellule composée de trois auteurs principaux opérait à Berne selon le même mode opératoire. Ils procédaient toujours de la même façon: ils demandaient en ligne, auprès de la même banque suisse, un crédit privé compris entre 25'000 et 80'000 francs au nom de complices. Les demandes de crédit comportaient des informations mensongères sur les revenus et la solvabilité des preneurs de crédit et s'accompagnaient de décomptes de salaire et d'extraits du registre des poursuites qui avaient été falsifiés. Parfois, les criminels indiquaient également une date de naissance erronée et transmettaient à la banque de fausses pièces d'identité afin que les preneurs de crédit mentionnés ne puissent pas être identifiés dans les bases de données grâce à leur date de naissance. Dès que les crédits étaient approuvés et versés, les criminels retiraient les montants en espèces. Lorsque les tentatives d'escroquerie se firent plus fréquentes, la banque procéda à un contrôle approfondi des documents remis et, pour plusieurs des infractions dénoncées, refusa le paiement du crédit. Dans son réquisitoire, le ministère public avait également demandé la condamnation d'un des criminels pour blanchiment d'argent, arguant que cette personne avait retiré en espèces, grâce à une procuration de compte, un crédit de 74'000 francs demandé au nom de son frère, puis en avait versé une partie sur un compte libellé à son propre nom dans une autre banque. Le prévenu avait utilisé l'intégralité de la somme à des fins personnelles. Le tribunal l'a cependant acquitté du grief de blanchiment d'argent. Le prévenu a été condamné à une peine privative de liberté de trois ans, dont 24 mois avec sursis. De plus, la banque lésée lui a réclamé des dommages-intérêts au civil.

d) Escroquerie à l'assurance

Lors d'une escroquerie à l'assurance, les criminels obtiennent le paiement d'une somme d'assurance sur la base de conditions erronées. Ces escroqueries peuvent être commises aussi bien contre des entreprises d'assurance privées que contre des autorités publiques. Si les auteurs n'agissent pas astucieusement, ils sont poursuivis en vertu de l'art. 148*a* CP, qui punit l'obtention illicite de prestations d'une assurance sociale ou de l'aide sociale d'une peine privative de liberté d'un an au plus. Par ailleurs, plusieurs lois fédérales relevant du droit des assurances sociales et des actes cantonaux (p. ex. sur l'aide sociale) ont leurs propres dispositions pénales[74]. En tant que délits ou contraventions, toutes ces infractions ne constituent toutefois pas un préalable au blanchiment d'argent. La tromperie astucieuse d'une assurance peut cependant réunir les conditions d'une escroquerie au sens de l'art. 146 CP. Elle peut être commise tant par les assurés que par un prestataire (p. ex. un médecin qui envoie à l'assurance de son patient des factures pour des prestations fictives ou excessives). Selon la configuration, les faits constitutifs d'escroquerie sont abandonnés par manque d'identité matérielle (cf. point 4.2). Lorsqu'un preneur de leasing déclare le vol de son véhicule en leasing couvert par une assurance casco pour se libérer du paiement des mensualités, il ne commet pas une

[74] Cf. art. 87 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS; RS 831.10); art. 76 de la loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP; RS 831.40); art. 92 de la loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal; RS 832.10); art. 31 de la loi fédérale du 6 octobre 2006 sur les prestations complémentaires à l'AVS et à l'AI (LPC; RS 831.30); art. 105 de la loi fédérale du 25 juin 1982 sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité (LACI; RS 837.0); art. 23 de la loi fédérale du 24 mars 2006 sur les allocations familiales (LAFam; RS 836.2) en relation avec l'art. 87 LAVS; art. 25 de la loi fédérale du 24 septembre 1952 sur les allocations pour perte de gain en cas de service et de maternité (LAPG; RS 834.1) en relation avec l'art. 87 LAVS; art. 70 de la loi fédérale du 19 juin 1959 sur l'assurance-invalidité (LAI; RS 831.20) en relation avec l'art. 87 LAVS.

escroquerie à l'assurance, mais éventuellement une atteinte astucieuse aux intérêts pécuniaires d'autrui au sens de l'art. 151 CP[75].

Lors d'une étude menée en 2017 sur mandat de l'Association Suisse d'Assurances (ASA), près de 10 % des personnes interrogées ont admis qu'elles-mêmes ou un autre membre de leur ménage avaient déjà fait valoir au moins une fois des frais non engagés ou engagés dans une proportion moindre auprès d'une assurance[76]. Les escroqueries concernaient principalement les assurances ménage et responsabilité civile privée. Nombre de ces cas seraient toutefois considérés comme une obtention illicite de prestations d'assurance au sens de l'art. 148*a* CP ou comme des infractions d'importance mineure, de sorte qu'une infraction de blanchiment d'argent est exclue d'emblée.

e) Fraude alimentaire

Les pratiques frauduleuses relatives aux denrées alimentaires font régulièrement les gros titres. Elles vont du restaurateur local qui sert à ses clients de la viande de cheval en prétendant que c'est du bœuf aux fraudes de grande envergure commises par des organisations criminelles[77]. Ces pratiques se déroulent tout le long de la chaîne alimentaire, et concernent notamment la vente de denrées de qualité inférieure, contrefaites ou falsifiées.

Les contrôles aléatoires laissent entrevoir un nombre considérable de cas non détectés. Du point de vue juridique, compte tenu du lien de causalité et de l'identité matérielle, les entreprises intermédiaires (en général, les grossistes ou le commerce de détail), et non les consommateurs finaux, sont souvent lésées en cas de fraudes alimentaires d'envergure impliquant des chaînes d'approvisionnement complexes. Si les caractéristiques de l'escroquerie ne sont pas réunies, et notamment l'astuce, les pratiques frauduleuses sont poursuivies, selon le cas, en tant que tromperie au sens de l'art. 64 de la loi sur les denrées alimentaires (LDAl)[78] ou en tant que falsification de marchandises selon l'art. 155 CP[79]. La tromperie au sens de la LDAl est une contravention et la falsification non qualifiée de marchandises, un délit; toutes deux ne constituent dès lors pas une infraction préalable au blanchiment d'argent[80].

Depuis 2011, Europol et Interpol coordonnent les opérations OPSON pour lutter contre la fraude alimentaire. La Suisse a participé à trois d'entre elles depuis 2017 (OPSON VI, OPSON VII et OPSON VIII). Les enquêtes portaient sur les céréales biologiques provenant d'Europe de l'Est (OSPON VI en association avec une campagne de contrôle nationale), la coloration du thon pour le rendre plus appétissant (OPSON VII) et l'étiquetage du café (OPSON VIII). Respectivement 4 % (coloration du thon) et 5 % (étiquetage du café) des échantillons suisses

---

[75] Stefan Maeder / Marcel Alexander Niggli (2019): *Art. 146* dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2e édition, Bâle, 2019, p. 3053; ATF 134 IV 210.
[76] ASA (2017): escroquerie à l'assurance: chiffres et faits. Résumé des résultats de l'étude GfK sur la fraude à l'assurance. 31 août 2017, p. 5, https://www.svv.ch/sites/default/files/2017-11/ASA%20re%CC%81sume%CC%81%20des%20re%CC%81sultats%20de%20l%27e%CC%81tude%20GFK%20sur%20la%20fraude%20a%CC%80%20l%27assurance%202017.pdf.
[77] Cf. p. ex. RFI (2012): Italie: un scandale qui mêle mafia et mozzarella. 17 juillet 2012. http://www.rfi.fr/fr/europe/20120717-italie-arrestation-plus-gros-producteur-mozzarella-bufflonne-lie-mafia; RTS (2013): Du cheval à la place de bœuf dans des tartares servis en Suisse. https://www.rts.ch/info/suisse/5329304-du-cheval-a-la-place-de-boeuf-dans-des-tartares-servis-en-suisse-.html.
[78] Loi fédérale du 20 juin 2014 sur les denrées alimentaires et les objets usuels (RS 817.0).
[79] Cf. art. 3 et 23 de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale (RS 241); Conseil fédéral (2011): message du 25 mai 2010 relatif à la loi fédérale sur les denrées alimentaires et les objets usuels, FF 2011 5181, 5252.
[80] Faire métier de la falsification de marchandises (art. 155, al. 2, CP) constitue toutefois un crime et peut dès lors être considéré comme une infraction préalable au blanchiment d'argent.

et liechtensteinois examinés étaient soupçonnés d'être frauduleux[81]. Des irrégularités sont régulièrement constatées (p. ex. dans la commercialisation du miel[82] ou découverte de pesticides dans des céréales prétendument biologiques et des produits de minoterie issus de plusieurs pays d'Europe de l'Est[83]). En Suisse, les fraudes dans le secteur alimentaire occasionneraient chaque année des dommages se chiffrant en millions. Dans l'Union européenne (UE), les coûts économiques découlant, pour l'industrie, de pratiques frauduleuses dans le domaine alimentaire sont estimés entre 8 et 12 milliards d'euros[84]. Seuls quelques rares cas font l'objet d'enquêtes; la fraude passerait souvent inaperçue. Il est cependant probable que des fonds incriminés provenant de ces fraudes alimentaires soient blanchis en Suisse. Une estimation plus approfondie de leur ampleur n'est toutefois pas possible, car les données à ce sujet font défaut.

f) Autres phénomènes d'escroquerie

Comme indiqué précédemment, il n'est pas possible d'établir une liste exhaustive des formes d'escroquerie en raison de la dynamique de ce domaine. D'autres phénomènes d'escroquerie visent régulièrement les entreprises, mais ils ne devraient constituer, au plus, qu'un risque très marginal de blanchiment d'argent pour la Suisse.

- *Escroquerie d'hôtel:* l'auteur se présente avec de faux documents et quitte l'hôtel sans payer le séjour. Un blanchiment d'argent subséquent semble plutôt improbable, car il n'y a aucun actif à blanchir.
- *Escroquerie au jeu*: les éléments du jeu (cartes, dès, etc.) sont truqués ou des billets de loterie (ou similaires) falsifiés ou non valables sont présentés. Ces infractions devraient être plutôt rares et concerner principalement des actifs de faible valeur.
- *Escroquerie au chèque*: l'auteur utilise des chèques (ou similaires) contrefaits, falsifiés, volés ou sans provision. Compte tenu du désintérêt croissant pour les chèques en tant que moyen de paiement, ce type d'escroquerie devrait être de plus en plus rare[85]. Entre 2009 et 2018, le MROS a reçu au total 39 communications de soupçons de blanchiment d'argent en relation concernant l'utilisation de chèques en lien avec une escroquerie comme infraction préalable présumée. Au demeurant, les escroqueries au chèque peuvent également viser des particuliers.
- Grâce à une *usurpation d'identité*, les escrocs utilisent le nom et l'adresse de personnes existant réellement pour commander des biens. Ils réceptionnent ensuite la livraison au domicile de l'acheteur présumé. En général, ce dernier ne découvre l'usurpation d'identité que lorsqu'il reçoit une facture pour des biens qu'il n'a jamais com-

---

[81] Cf. Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2018a): OPSON VII: a-t-on coloré le thon pour le rendre plus appétissant? Avril 2018. https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-eu-opson-thunfisch.pdf.download.pdf/Schlussbericht_OPSON_VII_FR.pdf; Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2019): OPSON VIII: vérification de l'étiquetage du café. Juin 2019. https://www.newsd.admin.ch/newsd/message/attachments/57404.pdf.

[82] Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2016): campagne nationale de détection des pratiques frauduleuses dans la commercialisation des miels et des poissons. https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/zusammenfassung-bericht-nat-kontrollprogramm-betrug-honig-fisch.pdf.download.pdf/Rapport_pour_le_public,_campagne_authenticit%C3%A9_miels_et_poissons,_R%C3%A9sum%C3%A9_F_2.pdf.

[83] Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2018b): rapport annuel 2017 sur les programmes de contrôle à la frontière. Surveillance des denrées alimentaires végétales et des objets usuels. https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-grenzkontrollen-2017.pdf.download.pdf/Jahresbericht_Kontrollprogramme_an_der_Grenze_2017_zu_pflanzl._LM_und_GG_FR.pdf.

[84] Commission européenne (2018): Knowledge Centre for Food Fraud and Quality. Infographic, https://ec.europa.eu/knowledge4policy/sites/know4pol/files/a0infographic_kc_food_fraud_final_0.pdf.

[85] Cf. Der Bund (2016): Der Check als Auslaufmodell. 23 juin 2016. https://www.derbund.ch/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/17304703.

mandés ni reçus. Sur le plan juridique, la personne directement lésée est le fournisseur, et non l'auteur supposé de la commande. Il est cependant difficile pour ce dernier de prouver son innocence au fournisseur.

- *Escroquerie à l'embauche*: un chercheur d'emploi se fait engager à la suite d'une tromperie astucieuse. Même s'il pourrait théoriquement y avoir de nombreux cas, ce type d'escroquerie devrait rarement être jugé par un tribunal pénal dans la pratique, car une solution de droit civil (licenciement immédiat, etc.) est plus appropriée. Celle-ci s'appliquerait également aux *escroqueries au temps de travail*, dans lesquelles un collaborateur saisit intentionnellement, dans le but de s'enrichir, un nombre d'heures de travail supérieur à celui qui a réellement été effectué.

3.2.3 Phénomènes d'escroquerie visant les particuliers

De par leur nombre, les particuliers constituent le plus grand groupe de victimes potentielles. Ils peuvent également être lésés par certains phénomènes susmentionnés, en particulier en qualité de créanciers privés en cas de banqueroutes frauduleuses, d'escroqueries au chèque ou d'hameçonnages en vue de l'utilisation frauduleuse d'un ordinateur. De plus, les escroqueries sur les sites de vente en ligne et les portails immobiliers, les escroqueries au placement ou à l'avance de frais, les prestations d'aide trompeuses, les escroqueries au change, les fausses demandes de soutien, les escroqueries au mariage et celles au prêt comptent parmi les phénomènes ciblant le plus souvent des particuliers.

a) Escroquerie sur les sites de vente en ligne et les portails immobiliers

Le négoce de biens et de services sur Internet offre aux criminels différentes possibilités d'escroquerie. Même les entreprises se laissent berner par des offres trompeuses. Les manœuvres suivantes ont été constatées fréquemment en Suisse:

- Les criminels proposent, sur des *magasins en ligne frauduleux*, des biens de grande marque à des prix exceptionnellement bas. Les marchandises commandées et payées n'arrivent cependant jamais chez les acheteurs ou se révèlent être des contrefaçons ou de piètre qualité. La grande majorité de ces magasins en ligne sont exploités depuis l'étranger et généralement calqués sur des sites de vente réels. Parfois, les escrocs utilisent également des sites reconnus de vente aux enchères sur Internet pour proposer des biens qu'ils ne possèdent absolument pas. Lorsque ces sites Web sont hébergés en Suisse, fedpol peut demander la suppression des contenus frauduleux en fournissant à l'hébergeur les références des pages concernées. En général, les sites de vente frauduleux qui sont supprimés réapparaissent néanmoins rapidement sous un autre nom.
- Les escrocs publient sur des portails immobiliers de *fausses annonces* pour des logements souvent fictifs ou qui ne sont pas à louer. Les personnes intéressées sont ensuite contactées, car leur dossier aurait été retenu. Les criminels demandent cependant le paiement préalable d'une caution. Ils disparaissent dès que celle-ci a été versée.
- Les criminels proposent à la victime, par l'intermédiaire d'une *société de transport fictive*, de lui livrer un bien commandé préalablement sur un portail de petites annonces. Cette société prend ensuite contact avec la victime et exige le paiement préliminaire des frais de transport ou du prix de vente. Une fois le paiement exécuté, les escrocs disparaissent dans la nature et le bien n'est jamais livré.
- En l'espèce, les criminels utilisent de *fausses confirmations de paiement* et se font passer pour des acheteurs. Ils envoient au vendeur un faux courriel du prestataire de paiement sélectionné, qui confirme que le paiement a été exécuté ou suspendu jusqu'à ce que l'envoi de l'article soit prouvé. Le vendeur expédie le bien acheté, mais ne reçoit aucune contrepartie.

En 2015, 8,5 % des personnes interrogées dans le cadre de l'étude de Biberstein et al. avaient été victimes d'un acte frauduleux en tant que consommateurs au cours des cinq années précédentes[86]. Plus d'un quart des cas (28,6 %) concernaient des achats sur Internet. Réalisées lors de l'étude de Beaudet-Labrecque et al., des extrapolations sur la prévalence de ces manœuvres estimaient en 2018 que près de 120'000 personnes de 55 ans et plus avaient été victimes d'annonces trompeuses sur Internet ces dernières années et presque 100'000, d'une escroquerie lors de processus de paiement en ligne. Parmi elles, près de 50'000 (annonces trompeuses) et plus de 10'000 (paiements en ligne) avaient subi un dommage financier[87]. En 2018, fedpol a enregistré 183 communications de soupçons de cybercriminalité portant sur de fausses annonces immobilières, 267 relatives à des magasins en ligne frauduleux, 260 concernant des contrefaçons et 63 sur des sociétés de transport fictives.

Plus de 10'000 escroqueries par an sont probablement commises sur les portails immobiliers et les sites de vente en ligne. Les montants moyens en question devraient être relativement faibles et se chiffrer, pour la plupart, en centaines de francs. Lorsque les criminels agissent par métier ou que le dommage dépasse 300 francs, il y a en général un acte de blanchiment d'argent.

Exemple d'escroquerie sur les sites de vente en ligne

Pendant une courte période, le prévenu avait mis son compte dans une banque suisse à la disposition d'une personne non identifiée, à la demande de cette dernière. Il a réceptionné six paiements d'un montant total de 2'260 francs et a transféré au moins une partie de cette somme à son donneur d'ordre par l'intermédiaire d'un établissement de transfert de fonds, bien qu'il ait pensé que les actifs étaient d'origine criminelle. Les fonds provenaient de plusieurs escroqueries sur Internet. L'instigateur et escroc proposait à la vente des smartphones et des sacs à main, même s'il n'a jamais eu l'intention de livrer les biens après la réception des paiements. Le prévenu a été condamné par ordonnance pénale pour blanchiment d'argent à 240 heures de travail d'intérêt général. N'ayant pas été identifié, l'escroc n'a pas pu répondre de ses actes.

Exemple d'escroquerie sur les portails immobiliers

Au printemps et à l'été 2015, A et B, deux criminels domiciliés à l'étranger, ont tenté de publier plus de 200 annonces d'appartement sur différents portails immobiliers suisses. À cette fin, ils ont séjourné plusieurs jours et sous de faux noms dans des hôtels de Zurich. Les gestionnaires des portails ont identifié la plupart de ces annonces comme étant frauduleuses et ne les ont pas mises en ligne. Néanmoins, 65 ont échappé à ces contrôles et ont été publiées. Plus de 2'000 personnes se sont déclarées intéressées. Les deux escrocs, qui utilisaient notamment des comptes utilisateur et e-mail falsifiés, ont pris contact avec elles en se faisant passer pour le propriétaire du logement. Ils leur annonçaient que leur dossier avait été retenu, et demandaient le paiement préalable d'un mois de loyer et d'une caution de plus de 2'000 francs en moyenne. Au final, onze personnes ont été piégées et ont viré l'argent sur un compte en Angleterre contrôlé par un agent financier. Les criminels ont ainsi pu faire main basse sur des actifs d'une valeur totale de 23'350 francs. L'un d'entre eux a également obtenu 3'750 livres sterling grâce à la vente frauduleuse d'un jet ski en réalité fictif sur un site de vente en ligne. En mars 2017, le tribunal de district de Zurich a condamné les deux escrocs pour escroquerie par métier, faux dans les titres, blanchiment d'argent et concurrence déloyale à une peine privative de liberté de respectivement trois ans et six mois et trois ans et trois mois.

b) *Escroquerie au placement*

Lors d'une escroquerie au placement, les escrocs tentent d'inciter les victimes potentielles à investir en leur promettant des gains élevés. Les fonds ou d'autres actifs ne sont pas placés

[86] Biberstein et al. (2016), référence susmentionnée, p. 16 et 17.
[87] Beaudet-Labrecque et al. (2018b), référence susmentionnée.

(ou ils ne le sont que partiellement), mais servent à enrichir les criminels. D'innombrables variantes de ce phénomène existent:

- Beaucoup d'escroqueries s'appuient sur un système de répartition (également appelé *système de Ponzi*[88]) dans lequel tout ou, du moins, une grande partie des rendements dépend de l'arrivée de nouveaux investisseurs. Tout le système s'effondre lorsque l'on ne parvient plus à trouver des nouveaux investisseurs en nombre suffisant. Ces escroqueries peuvent s'étendre sur plusieurs années et, dès lors, occasionner des dommages se chiffrant en millions. Le système de Ponzi est souvent confondu avec les *systèmes boule de neige et les systèmes pyramidaux*. Dans ces derniers, les participants tirent généralement avantage de l'enrôlement de nouveaux clients[89]. Ils savent que leur gain en dépend, ce qui n'est d'ordinaire pas le cas dans un système de Ponzi. Selon les circonstances, les systèmes boule de neige et les systèmes pyramidaux peuvent également être considérés comme une escroquerie[90].
- Le *boiler room*, soit le négoce frauduleux d'actions, est un autre type d'escroquerie au placement. La plupart du temps, les criminels tentent de convaincre par téléphone les victimes potentielles d'investir dans des actions (fictives). Ils agissent en général depuis des centres d'appels à l'étranger. L'expression *boiler room* reflète tant l'agitation qui y règne que la pression exercée sur les victimes. Contrairement à un système de répartition, ces dernières ne perçoivent aucun rendement ou uniquement des rendements très faibles pour les tenir en haleine.
- Une autre forme d'escroquerie au placement, les *initial coin offerings* (ICO) frauduleuses, concerne les cryptomonnaies. Comme lors d'une levée de fonds, les développeurs recherchent dans le cadre d'une *initial coin offering* les capitaux nécessaires au lancement de leur nouvelle cryptomonnaie ou idée commerciale. Les investisseurs mettent des moyens financiers à la disposition de l'organisation de l'ICO et reçoivent en contrepartie des *token* (ou jetons) de la nouvelle monnaie. L'*ICO exit scam* est une forme frauduleuse d'ICO: les criminels prétendent fonder une nouvelle entreprise et lever des fonds par l'intermédiaire d'une ICO. Ils disparaissent ensuite avec les fonds investis sans fournir aux investisseurs une contrevaleur pour leurs placements[91].

Dans la plupart des escroqueries au placement, les criminels affirment investir dans des startups ou dans la recherche médicale ou opérer dans le négoce d'actions, de fonds, de métaux précieux, de denrées alimentaires exotiques, d'énergies renouvelables, de matières premières, de devises, de biens immobiliers ou de crypto-actifs, et avoir développé un système révolutionnaire dont la fiabilité permet de générer des rendements élevés. En réalité, les moyens financiers ne sont pas placés comme promis ou ne le sont que partiellement; ils servent à financer le style de vie généralement très dispendieux des escrocs. Dans de nombreux cas, les criminels s'appuient sur les expériences acquises dans la finance au cours d'activités précédentes. On constate parfois que les escrocs ont exercé légalement comme conseillers financiers et placé avec un certain succès les fonds de leurs clients pendant de nombreuses années. Ils se sont ainsi constitués un portefeuille de clients considérable, dont ils connaissent parfaitement la situation financière. Lorsque les criminels recherchent des investisseurs pour leur nouveau modèle d'affaires frauduleux, ils peuvent donc trouver sans grand effort leurs premiers investisseurs solvables dans ce portefeuille.

---

[88] Il tient son nom de Charles Ponzi, qui utilisa cette manœuvre en Amérique du Nord au début du XX^{e} siècle.
[89] Cf. Conseil fédéral (2009): message du 2 septembre 2009 concernant la modification de la loi fédérale contre la concurrence déloyale (LCD), FF 2009 5539, 5564.
[90] Tina Balzli (2018): *Art. 3 Abs. 1 lit. r*, dans: Reto Heizmann / Leander D. Loacker (éditeur): UWG Bundesgesetz gegen den unlauteren Wettbewerb. Kommentar. Zurich, 2018, p. 718 et 719.
[91] Cf. également GCBF (2018b): le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding, octobre 2018.

D'après une extrapolation réalisée dans le cadre de l'étude de Beaudet-Labrecque et al., un placement frauduleux aurait été proposé à plus de 200'000 personnes de 55 ans et plus en Suisse ces cinq dernières années et 4 % d'entre elles (env. 8'600 personnes) auraient subi une perte financière[92]. Il n'y a aucun chiffre sur la prévalence auprès des générations plus jeunes. Le nombre annuel de victimes d'une escroquerie au placement est probablement inférieur à 10'000 en Suisse. Les dommages financiers peuvent toutefois varier très fortement d'un cas à l'autre. Selon les données de fedpol, le *boiler room* a rapporté aux criminels au moins 91 millions de francs en Suisse entre 2010 et 2017, mais les sommes effectivement dérobées devraient être plus élevées, car de nombreux cas ne sont vraisemblablement pas dénoncés. Le montant du dommage par victime fluctue énormément et va de quelques milliers de francs à plusieurs millions. Concernant les ICO frauduleuses, le réseau Ethereum[93] est particulièrement exposé, car 82 % des ICO sont exécutées sur sa *blockchain*. De plus, les ICO prenant la forme d'investissements décentralisés ont eu tendance à augmenter en 2017 et en 2018[94]. La plupart des escroqueries au placement qui réussissent, y compris celles impliquant des crypto-actifs, donnent probablement lieu à des actes de blanchiment d'argent.

Exemple d'escroquerie au placement

Pendant plus de 20 ans, le Texan Allen Stanford a géré aux États-Unis un système d'escroquerie au placement de très grande ampleur, que seul le système de Bernard Madoff a détrôné jusqu'à présent. La vente de certificats de dépôt (certificates of deposit) qui, d'après les promesses de Stanford, offraient des rendements annuels garantis d'au moins 10 % lui a permis de récolter des capitaux de l'ordre de 8 milliards de dollars, le versement des rendements étant financé par les avoirs des nouveaux clients. À l'aide d'un petit comité de direction composé de membres de sa famille et d'amis proches, Allen Stanford a mis en place un réseau d'entreprises international complexe, dont faisait partie la société Stanford Group (Suisse) AG domiciliée en Suisse. En 2012, Allen Stanford a été condamné aux États-Unis à une peine de prison de 110 ans.

Fondée en 1997 et domiciliée à Zurich jusqu'à sa liquidation, Stanford Group (Suisse) AG opérait principalement dans le conseil patrimonial et la gestion de fortune d'après son inscription au registre du commerce. Après l'ouverture, aux États-Unis, d'une procédure contre Allen Stanford et ses collaborateurs en 2009, le MROS a reçu plusieurs communications d'intermédiaires financiers suisses qui entretenaient des relations de compte avec Stanford Group (Suisse) AG. Le ministère public de la Confédération (MPC) a donc ouvert une procédure pour blanchiment d'argent et bloqué des actifs dépassant les 200 millions de francs suisses. Quelques mois après l'ouverture de la procédure aux États-Unis, le conseil d'administration de Stanford Group (Suisse) AG décida la liquidation ordinaire de l'entreprise. Le MPC a clôturé ses enquêtes correspondantes en 2014. Avec le soutien des autorités judiciaires américaines, il a découvert qu'une partie des fonds déposés en Suisse provenait de l'escroquerie au placement réalisée aux États-Unis. Comme les principaux prévenus devaient déjà répondre de leurs actes dans ce pays, la procédure suisse à leur encontre a été clôturée. En revanche, le MPC a condamné Stanford Group (Suisse) AG pour blanchiment d'argent qualifié à une amende d'un million de francs suisses par ordonnance pénale et en application de la responsabilité de l'entreprise au sens de l'art. 102, al. 2, CP. Il a également fixé une créance compensatrice qui s'inscrit dans la tranche supérieure des montants à sept chiffres pour les gains d'origine délictueuse. L'amende et la créance compensatrice ont bénéficié aux victimes de l'escroquerie au placement[95]

[92] Beaudet-Labrecque et al. (2018b), référence susmentionnée.
[93] Ethereum est une fondation sise à Zoug qui, depuis 2015, promeut notamment le protocole Ethereum basé sur la technologie *blockchain*. La cryptomonnaie d'Ethereum s'appelle Ether (ETH).
[94] Chainalysis (2019): Crypto Crime Report. Decoding Hacks, Darknet Markets, and Scams, p. 16. https://blog.chainalysis.com/.
[95] Ministère public de la Confédération (2014): la Suisse indemnise les lésés dans l'affaire Allen Stanford, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-52261.html.

c) *Fausse demande de soutien*

Lors d'une fausse demande de soutien, les criminels se font passer pour une connaissance de la victime et prétendent avoir urgemment besoin d'argent. Il existe de nombreuses variantes de cette escroquerie qui, selon le procédé, peuvent également être qualifiées d'escroquerie à l'avance de frais.

- L'une des variantes les plus connues est le *coup du neveu*. Les criminels se font passer pour des parents ou des proches de la victime et prétendent être dans une situation financière difficile. Si la victime est disposée à apporter une aide financière, le soi-disant parent ou proche prétexte ne pas pouvoir aller chercher l'argent personnellement à cause d'un rendez-vous. Au lieu de cela, il envoie une prétendue personne de confiance pour réceptionner le montant en espèces. Le coup du neveu est une variante d'une escroquerie téléphonique visant les particuliers.
- Dans la cybervariante, les criminels accèdent aux comptes e-mail de tiers, en général grâce à l'hameçonnage, et envoient en leur nom de fausses demandes de soutien à leurs contacts. Ils affirment, par exemple, avoir été victimes d'une agression à l'étranger et avoir perdu tout leur l'argent ainsi que leurs papiers d'identité. Ils demandent une aide financière et promettent de la rembourser dès leur retour. Généralement, les victimes sont priées d'envoyer l'argent via un établissement de transfert de fonds, car c'est la solution la plus rapide.
- Les fausses demandes de soutien peuvent également être réalisées de manière classique, c'est-à-dire sans l'aide d'Internet. Les criminels racontent une prétendue situation d'urgence aux victimes (p. ex. enfants gravement malades) et demandent de l'argent.

Les enquêtes policières ont révélé que les escrocs pratiquant le coup du neveu sont très bien organisés et se répartissent le travail. On estime que quelques milliers d'entre eux sont actifs au niveau européen, la plupart provenant d'Europe du Sud et d'Europe centrale.

D'après l'étude de Beaudet-Labrecque et al., il y aurait en Suisse plus de 20'000 tentatives de coup du neveu par an, dont 400 se solderaient par une perte financière[96]. Depuis 2011, fedpol a connaissance, en moyenne, de 600 tentatives par an, dont près de 10 % réussiraient du point de vue des criminels. Le montant moyen du dommage par cas déclaré s'inscrit à 45'000 francs. S'il est couronné de succès, le coup du neveu devrait fréquemment être suivi d'un acte de blanchiment d'argent, car les criminels passent généralement la frontière avec les fonds en espèces. Il n'existe en Suisse aucune estimation du nombre de fausses demandes de soutien effectuées sur Internet. Chaque année, fedpol reçoit quelques dizaines à quelques petites centaines de communications de soupçons de cybercriminalité qui portent sur cette variante du phénomène (2018: 21 communications de soupçons). Les sommes dérobées sont sensiblement inférieures au butin du coup du neveu et se chiffrent généralement à quelques centaines de francs.

d) *Prestations d'aide trompeuses*

Contrairement à une fausse demande de soutien, les criminels font croire à une situation d'urgence ou à une situation problématique chez les victimes dans le cas d'une prestation d'aide trompeuse. Les escroqueries impliquant un faux fonctionnaire de police ou de faux appels d'un centre d'assistance comptent parmi les variantes les plus fréquentes.

- Lors d'une *escroquerie avec un faux fonctionnaire de police*, les criminels se font passer pour des policiers et déclarent que l'argent ou les objets de valeur des lésés ne sont plus en sécurité pour différentes raisons. Un fonctionnaire de police viendra dès lors les chercher pour les mettre en sécurité.

[96] Beaudet-Labrecque et al. (2018b), référence susmentionnée.

- Lors d'*appels frauduleux d'un centre d'assistance*, les criminels prétendent être des techniciens de Microsoft, d'Apple ou d'entreprises similaires. Ils essaient par différentes astuces d'accéder à distance à l'ordinateur de la victime pour en tirer un avantage financier. Selon le cas, ils demandent également le paiement d'honoraires de conseil pour avoir résolu un prétendu problème informatique ou proposent de conclure un abonnement d'assistance ou d'acheter des licences de logiciel.

D'après les sondages auprès des victimes, il y aurait chaque année en Suisse plus de 4'000 tentatives impliquant un faux fonctionnaire de police[97]. Ce phénomène a progressé ces dernières années. Les cas déclarés à fedpol (y c. les tentatives) sont passés de 29 en 2016 à 2'560 en 2018, le taux de réussite étant inférieur à 2 %. Le montant moyen du dommage par cas était relativement élevé et s'établissait à 105'000 francs. De plus, fedpol reçoit chaque année en ligne entre 200 et 500 communications de soupçons de cybercriminalité qui peuvent relever d'un appel frauduleux d'un centre d'assistance. Dans cette dernière variante, le montant du délit se chiffre toutefois généralement à quelques centaines de francs.

e) Escroquerie à l'avance de frais

Dans ce mode opératoire, les criminels envoient des courriels, des SMS, des messages instantanés – auparavant, également des lettres – dans lesquels ils promettent aux victimes potentielles des gains ou commissions élevés. Ils leur précisent cependant que des avances doivent être versées pour débloquer ces fonds. Ces promesses de gain sont basées sur des histoires inventées, dont les plus répandues sont:

- *un héritage important*: les criminels affirment que la victime a hérité d'une grosse somme. La libération de cette dernière nécessite toutefois le règlement des frais de notaire, de transactions, des impôts, etc. Les criminels promettent une partie de l'héritage en échange de la couverture de ces frais;
- *des avoirs sans nouvelle*: les criminels se présentent comme des employés d'une banque africaine qui ont identifié des avoirs sans nouvelle. Pour pouvoir s'approprier ces fonds, ils ont juste besoin qu'un partenaire à l'étranger mette son compte bancaire à disposition et soit en mesure de régler différents frais administratifs;
- *un gain au loto*: les victimes potentielles sont informées qu'elles ont gagné au loto. Des frais doivent toutefois être payés avant le versement de leur gain.

Lorsqu'une victime mord à l'hameçon, les criminels l'invitent à envoyer des documents personnels et à exécuter des paiements – en général, par l'intermédiaire d'établissements de transfert de fonds. Dès que les premiers frais ont été réglés, de nouveaux prétextes sont inventés pour demander de l'argent supplémentaire. Il n'est pas rare que des victimes suisses versent des milliers de francs sans jamais recevoir les gains promis.

Des enquêtes ponctuelles des autorités suisses de poursuite pénale ont montré que les groupes de criminels fonctionnent comme une sorte d'économie de marché parallèle, dans laquelle des services et des produits sont généralement négociés sur des forums Internet spécifiques (*crime as a service*). Par exemple, un premier criminel propose un réseau d'ordinateurs infectés pour envoyer des pourriels (*spams*). Un deuxième criminel rédige les textes et prend contact avec les victimes potentielles. D'autres criminels se spécialisent, quant à eux, dans l'élaboration de documents et actes falsifiés, qui peuvent être transmis aux victimes pour prouver l'existence d'un prétendu gain au loto ou héritage. Dès que les premières sommes sont versées, il faut également des personnes pour aller les retirer auprès des établissements de transfert de fonds et les remettre à des hommes de main. Les services de ces agents financiers sont eux aussi proposés sur des forums Internet. Enfin, les personnes ayant déjà répondu par le passé à des courriels frauduleux sont répertoriées sur des listes, qui seront à leur tour revendues dans l'espoir que ces personnes se laissent berner une deuxième fois.

[97] Beaudet-Labrecque et al. (2018b), référence susmentionnée.

Souvent, les différents prestataires de ces produits et services ne se connaissent que vaguement, voire pas tout, sur ces forums Internet et n'ont que des relations superficielles. Les réseaux fonctionnent de manière très souple: le choix des prestataires et l'achat des services sont réalisés en fonction des disponibilités.

Les tentatives d'escroquerie à l'avance de frais sont très fréquentes en Suisse, mais la plupart échouent. Dans l'étude de Beaudet-Labrecque et al., le taux de réussite dépassait à peine 2 % en 2018. Après extrapolation, cela représentait quelque 8600 personnes de 55 ans et plus qui avaient subi un dommage financier à cause de cette manœuvre au cours des cinq années précédentes[98]. Il n'existe pas de données similaires pour les autres classes d'âge.

Le nombre réel d'escroqueries réussies à l'avance de frais est probablement inférieur à 10'000 par an et la plupart des montants concernés devraient se chiffrer en centaines ou voire à quelques milliers de francs. Comme les criminels sont souvent à l'étranger, les fonds doivent généralement être transférés par des intermédiaires financiers. Il n'est pas rare de faire également appel à des agents financiers pour brouiller les pistes. La majorité des escroqueries à l'avance de frais qui aboutissent devraient donc s'accompagner d'actes de blanchiment d'argent (contre-exemple: cf. encadré).

Exemple d'escroquerie à l'avance de frais

Un établissement de transfert de fonds a signalé un soupçon de blanchiment d'argent, car un client avait exécuté en à peu près un an 53 virements d'une valeur totale de 14'324 francs à treize destinataires dans cinq pays différents. Les transactions ont été détectées lorsque le prévenu a effectué un virement à un destinataire qui avait déjà reçu des fonds d'un autre client par le passé. Le prévenu a été prié d'indiquer le motif des virements et de fournir des documents sur l'origine des fonds (décompte de salaire, relevé de compte, etc.), mais il a refusé de le faire. S'appuyant sur la communication de soupçons, le ministère public cantonal compétent a alors ouvert une procédure pour blanchiment d'argent contre le prévenu. Lors de son audition, celui-ci a finalement déclaré que les fonds envoyés en Espagne et dans plusieurs pays africains provenaient de ses propres ressources. Il avait cherché sur Internet des possibilités de gagner de l'argent et avait ensuite été contacté par des personnes étrangères qui lui avaient proposé des affaires dans lesquelles il devait toutefois verser des avances. Les enquêteurs ont rapidement constaté que le prévenu était victime d'une escroquerie à l'avance de frais. L'origine licite des fonds ayant pu être prouvée, la procédure engagée contre le prévenu pour blanchiment d'argent a été clôturée.

f) Escroquerie au change

Dans une escroquerie au change, les criminels essaient de faire participer la victime à une opération financière et, dans le cadre du règlement, d'échanger de la fausse monnaie contre de la vraie. Il existe différentes variantes:

- Lors d'un *rip deal*, les criminels essaient d'attirer des personnes avec des promesses de gains élevés pour les convaincre d'échanger – frauduleusement – des devises. Lors de la remise des fonds, voire lors d'une transaction en bitcoins, la victime est toutefois dépossédée de son argent, car elle reçoit en général de la monnaie sans valeur (faux billets, etc.). En fonction du déroulement, le *rip deal* sera plutôt considéré comme un vol. Les entreprises peuvent elles aussi faire partie des lésés.
- Lors d'une arnaque dite aux billets noirs ou au lavage d'argent (*wash-wash*), les criminels font croire à la victime qu'ils peuvent multiplier l'argent grâce à un liquide chimique ou laver des (présumés) billets de banque colorés. Une partie du gain est

[98] Beaudet-Labrecque et al. (2018b), référence susmentionnée.

promise à la victime, qui doit néanmoins verser une avance. Il existe plusieurs variantes de cette escroquerie; selon les circonstances, certaines peuvent être qualifiées d'escroquerie à l'avance de frais.

- Lors d'un simple *échange de devises*, on demande spontanément à la victime dans la rue si elle peut changer une monnaie étrangère. En contrepartie, le passant reçoit généralement de la fausse monnaie ou les criminels profitent de l'occasion pour voler de l'argent dans le portemonnaie, ce qui s'apparenterait alors à un vol par ruse.

En général, les escroqueries au change de type *rip deal* et *arnaque aux billets noirs*, principalement, sont attribuables au crime organisé. Concernant le *rip deal*, la plupart des faits sont commis par les mêmes grandes familles criminelles qui sont originaires d'Europe du Sud-Est et sont désormais établies dans la majorité des pays d'Europe méridionale et centrale. L'arnaque aux billets noirs est souvent réalisée par des groupes d'Afrique de l'Ouest. Dans les deux cas, les criminels agissent sur le plan international et se répartissent le travail.

D'après une extrapolation réalisée dans le cadre de l'étude de Beaudet-Labrecque et al., environ 170'000 personnes de 55 ans et plus ont été confrontées à un échange frauduleux de devises ces cinq dernières années et 23'000 d'entre elles auraient subi un dommage financier sur la même période[99]. Toutefois, celui-ci résulterait parfois d'un vol, et non d'une escroquerie. Chaque année, entre 20 et 50 cas de *rip deal* sont déclarés à fedpol, dont 10 à 20 ont mené à une perte financière. Le montant moyen du dommage par cas recensé dépasse 400'000 francs; il est donc relativement élevé. Il n'existe aucun chiffre global concernant l'*arnaque aux billets noirs*, mais ce type d'escroquerie devrait plutôt être un délit de niche. Comme les criminels passent souvent la frontière avec les fonds incriminés en espèces, un acte de blanchiment d'argent devrait également être exécuté la plupart du temps, à condition que l'escroquerie soit caractérisée. Si l'argent que la victime propose d'échanger provient d'un crime ou d'un délit fiscal qualifié, le *rip deal* serait alors considéré comme un acte de blanchiment d'argent (qui a échoué). En général, ces cas n'incitent pas les victimes – qui ne sont probablement pas si rares que cela – à porter plainte.

g) *Escroquerie au mariage (*romance scam*)*

Dans une escroquerie au mariage, le criminel feint une relation amoureuse pour en tirer un avantage financier. La variante réalisée sur Internet est souvent appelée *romance scam*. La prise de contact s'effectue sur des plateformes de rencontre en ligne, sur les réseaux sociaux, dans des forums de discussion, etc. Après un échange prolongé de courriels, de lettres ou au téléphone, les criminels tentent d'inciter la victime à transférer de l'argent. Les prétextes classiques sont, par exemple, une visite à la victime qui «tombera cependant à l'eau» à la dernière minute ou les prétendues complications médicales d'un parent qui nécessitent une rentrée d'argent urgente. Les virements sont souvent effectués grâce à des prestataires de paiement. L'escroc disparaît dès qu'il a atteint son objectif ou que la victime arrête les paiements. Des groupes organisés venant d'Afrique de l'Ouest se cachent fréquemment derrière ces manipulations. D'autres régions d'origine ont également été identifiées.

En 2018, l'étude de Beaudet-Labrecque et al. estimait que presque 40'000 personnes de 55 ans et plus avaient été victimes d'une tentative de *romance scam* au cours des cinq dernières années. Toujours d'après cette étude, 15'000 d'entre elles auraient subi une perte financière[100]. Le montant du dommage peut varier de manière considérable. Dans certains cas, il peut même atteindre plusieurs dizaines de milliers de francs. Il n'existe aucune donnée comparable pour les autres classes d'âge. Les fonds étant généralement transférés à l'étranger, une escroquerie au mariage réussie devrait souvent s'accompagner d'un acte de blanchiment d'argent.

[99] Beaudet-Labrecque et al. (2018b), référence susmentionnée.
[100] Beaudet-Labrecque et al. (2018b), référence susmentionnée.

h) Escroquerie au prêt

Contrairement à l'escroquerie au crédit, le criminel fait office de bailleur de fonds dans une escroquerie au prêt. Il promet un prêt à la victime, mais exige d'elle une commission d'intermédiation qui doit être versée au préalable. Dès que le paiement a été exécuté, l'escroc cesse tout contact sans avoir octroyé le moindre prêt.

fedpol ne dispose pas de chiffres fiables sur l'ampleur de ce phénomène. Le nombre annuel de cas pourrait se chiffrer à quelques centaines.

i) Obtention ou vente frauduleuse de marchandises

Lors de l'obtention ou de la vente frauduleuse de marchandises, des produits de mauvaise qualité, contrefaits ou falsifiés sont vendus ou des biens sont acquis frauduleusement par des criminels qui n'ont pas l'intention de les payer (concernant la fraude alimentaire et la variante sur les sites de vente en ligne, cf. les sections correspondantes précédentes). Ces cas sont assez fréquents. Beaucoup seraient toutefois considérés comme des infractions d'importance mineure contre le patrimoine et ne constitueraient donc pas une infraction préalable au blanchiment d'argent. Ces escroqueries peuvent également viser des entreprises.

L'*obtention ou la vente frauduleuse de véhicules* en est une variante particulière. Des véhicules loués, volés, manipulés ou défectueux sont vendus ou des véhicules sont acquis sans intention de les payer. Rendues publiques en 2015, les manipulations des émissions polluantes des véhicules du groupe allemand Volkswagen AG ont montré que des escroqueries potentielles dans ce domaine pouvaient rapidement prendre une grande ampleur. Depuis 2016, le MPC mène une procédure pénale contre Volkswagen AG en Allemagne, la société d'importation concernée en Suisse ainsi que ses organes et employés responsables pour suspicion d'escroquerie par métier. Il leur est reproché d'avoir lésé quelque 175'000 acheteurs de véhicules et preneurs de leasing tout en ayant eu partiellement connaissance de ces manipulations[101]. On ne saurait dire pour l'heure dans quelle mesure des actes de blanchiment d'argent ont eu lieu.

j) Autres phénomènes d'escroquerie

Le nombre de phénomènes d'escroquerie visant les particuliers ne saurait être indiqué de manière exhaustive. Compte tenu de leur fréquence, il convient de mentionner l'*escroquerie à la mendicité* et la *fraude aux dons*. Il en existe plusieurs variantes. Les criminels se font souvent passer pour des personnes handicapées et récoltent de l'argent pour des organisations caritatives généralement fictives. L'arnaque à l'essence est également répandue: les criminels attendent à côté de leur véhicule au bord d'une route et arrêtent les automobilistes en leur demandant de l'argent pour de l'essence, argent qui n'est jamais remboursé. Ces faits sont généralement traités comme des infractions d'importance mineure. Certains indices de la police laissent néanmoins penser qu'une partie des escroqueries à la mendicité et des fraudes aux dons en Suisse est bien organisée. Les actifs subséquents à blanchir seraient toutefois relativement modestes.

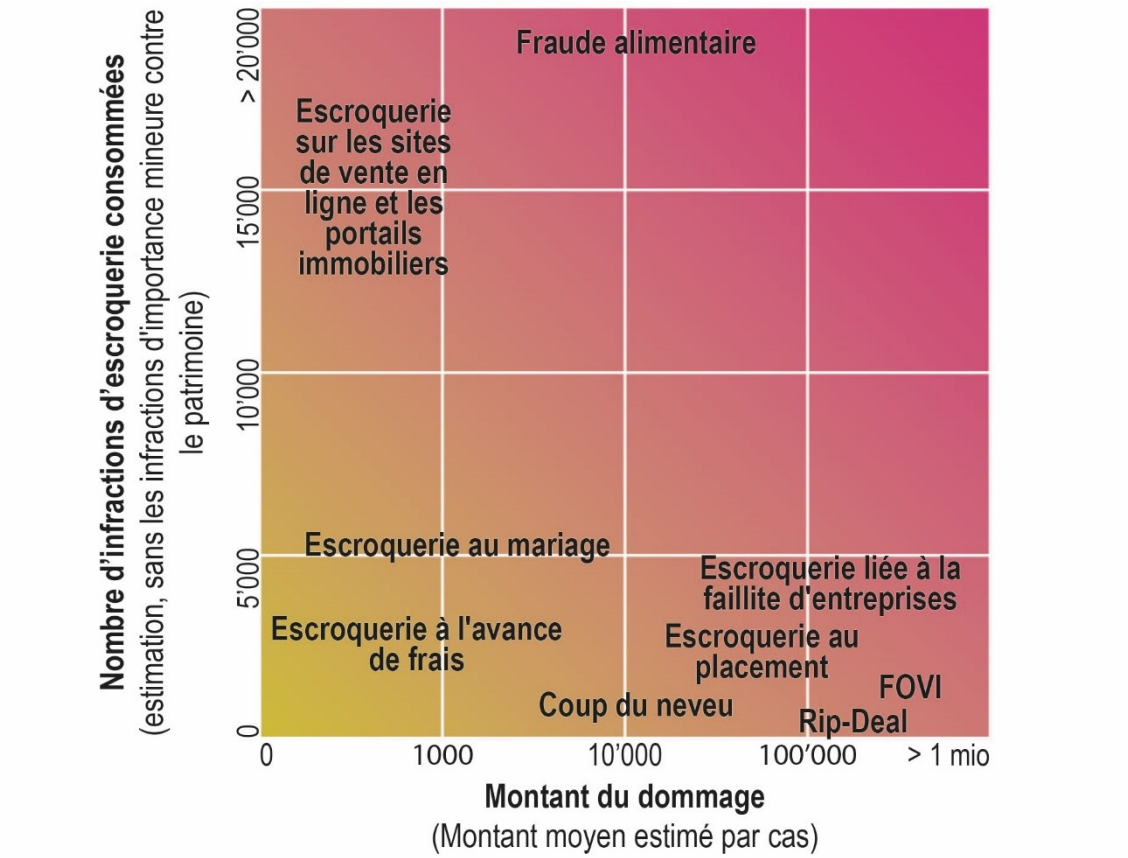
3.2.4 Évaluation des risques liés aux phénomènes d'escroquerie spécifiques

Les phénomènes d'escroquerie analysés présentent de grandes divergences. Ils visent des victimes ou groupes de victimes différents, requièrent des opérations plus ou moins complexes et affichent des réussites disparates. Quels que soient les procédés, il convient de souligner le rapport entre le nombre de victimes potentielles et les revenus pouvant être obtenus: d'une part, certaines escroqueries de masse nécessitent un travail relativement faible et rapportent en moyenne assez peu par cas. Les escroqueries sur les magasins en ligne ou les plateformes immobilières en sont des exemples typiques: le montant du dommage par victime se chiffrent

[101] Ministère public de la Confédération (2019): manipulations des émissions polluantes des véhicules du groupe VW: questionnaire en ligne pour les lésés. Communiqué de presse du 2 septembre 2019, https://www.bundesanwaltschaft.ch/mpc/fr/home/medien/archiv-medienmitteilungen/news-seite.msg-id-76267.html.

généralement en dizaines ou en centaines de francs. D'autre part, certains modes opératoires plus rares de par leur nombre génèrent des gains élevés pour les criminels. Ceux-ci doivent, en moyenne, investir davantage de temps, notamment pour les prestations d'aide trompeuses ou les faux ordres de virement. Dans ces formes d'escroquerie, le montant du dommage par cas atteint régulièrement plusieurs centaines de milliers de francs. Les fraudes dans le domaine alimentaire font figure d'exception: elles nécessitent un faible travail de réalisation et peuvent, selon les circonstances, produire des revenus criminels notables.

La menace potentielle est donc la plus élevée pour les formes d'escroquerie qui concernent un grand nombre de personnes ou occasionnent des dommages élevés par cas. Jusqu'à présent, on présume que ces deux critères se combinent uniquement dans la fraude alimentaire, mais les données correspondantes sont encore très lacunaires. Les faux ordres de virement internationaux, certaines escroqueries au change (notamment le *rip deal*) et de nombreuses escroqueries au placement affichent le plus fort risque potentiel de blanchiment d'argent par



Graphique 8: Infractions d'escroquerie selon l'estimation de leur fréquence et du montant de leurs dommages. Il n'existe aucune estimation pour certains phénomènes.

cas. Des montants assez conséquents sont dérobés, puis blanchis à cette occasion. Les escroqueries sur les sites de vente en ligne et les portails immobiliers représentent un risque accru, principalement en raison de leur nombre total. L'hameçonnage proprement dit ne pose aucun risque de blanchiment d'argent, car il n'affecte en général pas encore les actifs. Seuls ceux qui sont obtenus par la suite, la plupart du temps grâce à l'utilisation frauduleuse d'un ordinateur, constituent une infraction préalable au blanchiment d'argent. L'ampleur de cette menace est cependant difficile à estimer, car les données à ce sujet font défaut. Si l'on extrapole à l'échelle de la Suisse l'estimation des infractions liées aux faillites frauduleuses réalisée par les autorités pénales zurichoises, ce phénomène engendrerait chaque année des dommages supérieurs à 1 milliard de francs et serait donc, lui aussi, une menace potentielle majeure sur le plan financier. Globalement, le montant du dommage moyen est un peu plus élevé pour l'État et les entreprises que pour les particuliers.

4 Vulnérabilités et défis

Dans le cas des actes de blanchiment d'argent ayant comme infractions préalables l'escroquerie et l'utilisation frauduleuse d'un ordinateur, les vulnérabilités générales sont les mêmes que pour les autres infractions préalables. La Suisse ayant un secteur financier important, elle est exposée à une utilisation potentiellement abusive de sa place financière à des fins de blanchiment d'argent. Cela concerne également les actes correspondants dont l'infraction préalable est une escroquerie. Les rapports NRA déjà publiés ont cependant révélé qu'un système de lutte contre le blanchiment d'argent à la fois global, coordonné et efficace sur les plans juridique et institutionnel permettait de maîtriser les vulnérabilités générales d'un pays en la matière. C'est la raison pour laquelle celles-ci ne sont pas traitées plus avant ici; il est renvoyé à ces rapports NRA[102].

Ce chapitre est principalement consacré aux vulnérabilités spécifiques et à celles qui sont liées au dispositif institutionnel, car elles présentent certaines particularités concernant l'escroquerie et l'hameçonnage. Ces vulnérabilités constituent également un défi pour les autorités de poursuite pénale.

4.1 Vulnérabilités spécifiques

Les *vulnérabilités spécifiques* sont liées aux pratiques et instruments utilisés dans un secteur d'activités donné. Dans les escroqueries et l'hameçonnage, elles découlent principalement de l'utilisation du numéraire et de systèmes de virement informels, du recours à des agents financiers et à des personnes morales ayant leur siège à l'étranger ainsi que des possibilités accrues d'internationaliser les infractions pénales et le blanchiment d'argent connexe grâce aux dernières innovations informatiques. Les informations sur l'usage des crypto-actifs à des fins de blanchiment d'argent après des infractions d'escroquerie ou d'hameçonnage sont encore lacunaires; ces technologies comportent néanmoins une grande vulnérabilité potentielle.

4.1.1 Numéraire

Selon le rapport NRA sur l'utilisation du numéraire, le risque d'une utilisation abusive du numéraire à des fins de blanchiment d'argent en Suisse est modéré[103]. L'usage régulier du numéraire a toutefois été constaté dans les escroqueries et, en particulier, dans certaines escroqueries en ligne. Les cas analysés dans le présent rapport révèlent eux aussi que le numéraire est souvent employé pour certains phénomènes. Cela concerne notamment les escroqueries de type «coup du neveu» et «faux fonctionnaire de police» ainsi que l'escroquerie au change, dans lesquelles du numéraire, principalement, franchit physiquement la frontière. Dans les escroqueries numériques, les criminels tentent de brouiller les pistes en faisant appel à des agents financiers qui retireront l'argent transféré et le verseront sur de nouveaux comptes ou l'expédieront en espèces par voie postale (dans des enveloppes ou colis).

4.1.2 Systèmes de virement informels

Souvent, les systèmes de virement informels proviennent initialement de régions dans lesquelles le secteur bancaire n'est pas très bien établi ou ne fonctionne pas. Également utilisés pour des activités criminelles, ces systèmes (p. ex. hawala) s'appuient sur des mécanismes de compensation et se limitent en général à des groupes homogènes sur le plan ethnique, idéologique ou religieux. L'origine des fonds est d'autant plus difficile à établir qu'il n'y a aucune

[102] Cf. notamment GCBF (2018a): rapport sur l'utilisation du numéraire et les risques inhérents d'utilisation abusive pour le blanchiment d'argent et le financement du terrorisme en Suisse, octobre 2018.https://www.newsd.admin.ch/newsd/message/attachments/55178.pdf; GCBF (2018b), référence susmentionnée: https://www.newsd.admin.ch/newsd/message/attachments/55112.pdf; GCBF (2017): risque de blanchiment d'argent associé aux personnes morales, novembre 2017. https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-nov-2017-f.pdf; GCBF (2015a), référence susmentionnée.
[103] GCBF (2018a), référence susmentionnée.

transaction physique la plupart du temps, mais une compensation entre les différents «prestataires». Le recours à ces systèmes est supposé principalement pour le phénomène des faux ordres de virement internationaux, mais il n'a pas encore été prouvé.

4.1.3 Personnes morales ayant leur siège à l'étranger

Les entités juridiques commerciales étrangères présentent un risque de blanchiment d'argent plus élevé que leurs homologues suisses, quelle que soit la forme juridique[104]. Même les trusts peuvent être utilisés abusivement à des fins de blanchiment d'argent. Infraction préalable présumée parmi les plus fréquentes (première ou deuxième place du classement), l'escroquerie joue un rôle important pour les entités juridiques suisses et étrangères. Un système efficace de défense et de lutte, et notamment les obligations de diligence des intermédiaires financiers, peut cependant réduire considérablement ce risque pour les entreprises nationales.

En général, le lien entre des entités juridiques commerciales étrangères et la Suisse se résume aux comptes bancaires ouverts dans ce pays. D'après la statistique du MROS relative aux communications de soupçons (cf. point 3.1.4), 20 % des cocontractants sont des personnes morales étrangères dans les cas où l'escroquerie est une infraction préalable présumée (de 2016 à 2018). Plus des deux tiers (72 %) étaient des sociétés de domicile ayant principalement leur siège en Amérique centrale et aux Caraïbes (63 % des sociétés de domicile étrangères) ainsi qu'en Europe de l'Est (24 %). Les ayants droit économiques des sociétés de domicile se trouvent régulièrement dans une autre région du monde que leur société; il s'agit la plupart du temps de l'Europe de l'Est (27 % des ayants droit économiques lorsqu'une société de domicile est cocontractante), des États post-soviétiques (23 %) ainsi que du Proche et du Moyen-Orient (13 %). Cela confirme les soupçons selon lesquels les sociétés de domicile sont utilisées pour blanchir des fonds d'origine frauduleuse. Il existe une vulnérabilité spécifique lorsque ces sociétés sont domiciliées dans des États souvent peu coopératifs avec les autorités suisses de poursuite pénale.

4.1.4 Agents financiers

Le recours à des agents financiers, également appelés *money mules*, est un mode opératoire fréquent pour blanchir des fonds issus d'une escroquerie ou de l'utilisation frauduleuse d'un ordinateur. Les escrocs sont imaginatifs lorsqu'il s'agit de trouver des complices chargés de transférer les fonds dérobés. La plupart des personnes sont attirées par une offre d'emploi alléchante pour un poste d'agent financier, ce dernier devant exécuter le trafic des paiements depuis la Suisse pour de soi-disant entreprises internationales (qui opèrent souvent sur le marché immobilier). Les criminels se présentent plus rarement comme une organisation caritative recherchant des représentants en Suisse pour transférer les dons destinés aux enfants en détresse dans des régions en crise[105]. Dans certains cas, ils se font passer sur des sites de rencontre ou sur les réseaux sociaux pour des femmes d'Europe de l'Est désireuses de se marier et simulent une relation amoureuse avec des hommes suisses. En général, les escrocs essaient dans un premier temps de les inciter à transférer leur propre argent en vue d'un supposé voyage de la partenaire en Suisse. Si les victimes ne peuvent ou ne veulent pas le faire, ils prétendent alors qu'un parent éloigné pourrait fournir le montant requis, mais que l'agent financier devrait le virer depuis son propre compte. Étant donné que les établissements de transfert de fonds sont de plus en plus sensibilisés à cette problématique et refusent dès lors la transaction dans de nombreux cas, les agents financiers sont invités à expédier la somme, retirée en espèces, par l'intermédiaire d'une société internationale d'envoi de colis et de livraison express. En général, la commission promise va de 2 % à 10 % du montant à transférer. En réalisant ces activités, les agents financiers remplissent les conditions de l'état de fait objectif de blanchiment d'argent et risquent des poursuites pénales.

[104] GCBF (2017), référence susmentionnée.
[105] Office fédéral de la police fedpol (2011b), référence susmentionnée, p. 5.

Les sommes qui transitent par les agents financiers sont souvent relativement faibles (d'ordinaire, moins de 20'000 francs). Sur le plan quantitatif, elles représentent toutefois une part importante des communications de soupçons adressées au MROS et engendrent donc un travail considérable pour les autorités de poursuite pénale. De plus, l'analyse des décisions des tribunaux et des ministères publics révèle que les agents financiers sont acquittés dans certaines circonstances, car il n'y a pas d'intention délibérée. Par ailleurs, certains cas sont considérés comme des infractions d'importance mineure contre le patrimoine et ne constituent dès lors pas une infraction préalable au blanchiment d'argent[106].

Exemple d'agent financier

A a trouvé sur Internet une offre d'emploi de la société immobilière britannique XY, qui recherchait des responsables régionaux. D'après le contrat de travail envoyé à A par courriel, ses tâches consistaient notamment à réceptionner sur son compte les paiements exécutés par les clients en relation avec des opérations immobilières et à transférer l'argent par l'intermédiaire de sociétés d'envoi de colis et de livraison express. En contrepartie, elle pouvait conserver 3 % des montants virés. Début 2015, un criminel non identifié a exécuté, lors d'une attaque basée sur un maliciel, un virement de 7'630 francs depuis le compte d'un couple suisse vers le compte bancaire de A. Peu après, A a été contactée à deux reprises par une inconnue, qui l'a priée de retirer la somme reçue, après déduction de la commission, et de l'envoyer à Moscou, à une personne inconnue de A, via une société d'envoi de colis et de livraison express. La banque ayant identifié le virement à A comme potentiellement frauduleux et l'ayant bloqué, il n'y a eu qu'une tentative de blanchiment d'argent. A a été condamnée par ordonnance pénale à une peine pécuniaire ferme de 30 jours-amende de 30 francs chacun.

4.1.5 Internationalisation des infractions préalables frauduleuses et du blanchiment d'argent connexe

Les enquêteurs découvrent un lien international dans de très nombreuses procédures relatives à la criminalité économique. Internet permet à des criminels situés dans des pays éloignés de commettre des escroqueries en Suisse. Même lorsque le criminel et la victime se trouvent dans ce pays, de nombreuses enquêtes dévoilent des connexions internationales, par exemple lorsque les serveurs concernés sont hébergés hors de Suisse ou l'argent dérobé est transféré à l'étranger. Chaque escroquerie ou utilisation frauduleuse d'un ordinateur peut potentiellement avoir une ramification internationale. Cela vaut en particulier pour les cyber-escroqueries telles que l'hameçonnage, les escroqueries à l'avance de frais, les faux ordres de virement internationaux, les prestations d'aide trompeuses, les demandes de soutien ou les escroqueries au mariage (*romance scams*). De nombreuses escroqueries au placement ou au change présentent elles aussi des liens avec l'étranger. S'y ajoutent les infractions pénales commises à l'étranger et dont au moins une partie des fonds se trouvent en Suisse pour être blanchis par l'intermédiaire du système financier helvétique.

Les criminels travaillent très rapidement, changent régulièrement de fausses identités et font fi des frontières. Le traitement de ces cas sur le plan pénal nécessite des connaissances spécifiques en informatique, et les ressources requises sont extrêmement élevées. Cela tient notamment au fait que chaque délit correspondant présente un nombre de victimes relativement bas et des dommages assez faibles, qui se chiffrent en général en centaines ou, au plus, en milliers de francs. Même si des indices laissent penser qu'un même criminel est responsable, dans la plupart des cas, de toute une série d'infraction, il n'est guère possible d'en apporter la preuve. Dans quelques rares cas uniquement, les différentes infractions fourniront assez d'indices pour mettre à jour une structure plus importante.

[106] Les ministères publics et les corps de police traitent régulièrement des agents financiers au sein du Cyberboard (cf. point 1.3).

Lorsque des cas ont des ramifications internationales, les enquêteurs sont tributaires de l'entraide judiciaire internationale pour pouvoir éclaircir les faits. Les représentants interrogés des autorités de poursuite pénale déclarent que la coopération internationale dans le cadre de cette entraide prend parfois beaucoup de temps, mais que la plupart du temps ils obtiennent les informations recherchées. D'après l'expérience de ces autorités, les demandes d'entraide judiciaire aussi brèves et concrètes que possible donnent les résultats les plus prometteurs. La pratique a montré que les vérifications policières et l'échange d'informations entre les cellules de renseignements financiers (CRF) en amont des enquêtes de procédure pénale pouvaient décharger l'entraide judiciaire et en améliorer l'efficacité. Les informations recueillies dans le cadre de la coopération policière, c'est-à-dire en dehors de l'entraide judiciaire, ne sont pas recevables devant un tribunal et ne peuvent également pas être transmises à d'autres autorités sans l'accord de la CRF concernée. Sur la base de ces données, le ministère public peut cependant mener des enquêtes ciblées par la voie de l'entraide judiciaire, celles-ci servant ensuite de preuves dans les procédures suisses, en application de la loi sur l'entraide pénale internationale. Certains pays comme l'Allemagne ou la France disposent, par exemple, de registres centralisés des comptes bancaires. Ces registres ne comportent aucune information sur les soldes des comptes ou les transactions bancaires, mais indiquent uniquement si une personne détient une relation de compte bancaire dans le pays en question et auprès de quelle banque. Au niveau européen, la directive 2018/843 prévoit que les États membres mettent en place d'ici le 10 septembre 2020 des mécanismes automatisés centralisés, tels que des registres centraux ou des systèmes électroniques centraux de recherche de données, permettant l'identification, en temps utile, de toute personne qui détient ou contrôle des comptes de paiement et des comptes bancaires tenus par un établissement de crédit établi sur leur territoire. Les informations conservées dans ces mécanismes centralisés doivent être accessibles aux CRF nationales et aux autorités compétentes[107].

4.1.6 Crypto-actifs

Le risque découlant de l'utilisation de crypto-actifs ne peut pas être évalué précisément en raison du faible nombre de cas connus[108]. Le fait que les transactions soient souvent exécutées rapidement, sur le plan international et, pour la plupart, sans intermédiaire financier constitue toutefois une vulnérabilité majeure. En outre, il n'est guère possible sur le plan technique de saisir les actifs incriminés en l'absence de clé privée (*private key*). L'utilisation de services de mixing (également appelés *mixer* ou *tumbler*), qui mélangent fortement les actifs ou les répartissent entre plusieurs adresses cibles pour en dissimuler l'origine criminelle, complique les investigations. Jusqu'à présent, le recours aux crypto-actifs lors d'escroqueries concernait principalement les escroqueries au placement, notamment en lien avec les ICO (*exit scams*), avec certains systèmes boule de neige ou systèmes de Ponzi, ainsi que dans des *phishing scams*[109] et quelques cas de *rip deal*.

4.2 Vulnérabilités et défis liés au dispositif juridique et institutionnel

Les vulnérabilités liées au dispositif institutionnel découlent souvent du traitement juridique de l'escroquerie, qui constitue un défi pour les autorités de poursuite pénale. L'infraction pénale d'utilisation frauduleuse d'un ordinateur se révèle moins problématique à cet égard. Les vulnérabilités tiennent essentiellement aux éléments suivants: la pluralité des formes d'escroqueries et ses caractéristiques complexes, les délais de prescription différents de l'infraction préalable et du blanchiment d'argent, la preuve de l'infraction préalable, les différences de procédure en matière de blanchiment d'argent et d'escroquerie, la confiscation des actifs en temps opportun et, enfin, la non-identification d'une infraction pénale.

---

[107] Art. 32a de la directive européenne 2018/843 du 30 mai 2018.

[108] GCBF (2018b), référence susmentionnée.

[109] Variante de l'hameçonnage dans laquelle la victime est amenée à partager des informations permettant aux escrocs d'accéder à son *wallet* et donc à sa clé privée.

4.2.1 Pluralité des formes d'escroqueries

L'analyse des menaces a révélé qu'une escroquerie ou l'utilisation frauduleuse d'un ordinateur peuvent être exécutées de différentes façons. Cette diversité est une vulnérabilité, car elle complique l'identification, l'analyse et, au final, la poursuite pénale des infractions d'escroquerie. Par exemple, la question de l'astuce doit être posée pour chaque nouveau phénomène d'escroquerie.

Cette diversité ressort également des procédures analysées sur le plan qualitatif. L'évaluation a mis en lumière plusieurs modes opératoires. Cette polyvalence concerne non seulement le type d'acte criminel, mais aussi le dommage ou la durée de la procédure. Par exemple, cette dernière peut prendre fin au bout d'un mois déjà, tandis qu'une autre sera clôturée plus de douze ans après son ouverture. Dans les décisions de justice examinées, les procédures ont duré en moyenne à peine trois ans. Quant aux actifs incriminés, leur montant va de quelques centaines de francs à des dizaines de millions.

Les actes subséquents de blanchiment d'argent utilisent des modes opératoires qui sont également observés dans des procédures liées à d'autres infractions préalables. Dans les procédures examinées, les criminels ont surtout tenté de dissimuler la piste des fonds en virant l'argent entre plusieurs comptes en Suisse et à l'étranger. D'après les communications de soupçons au MROS, l'infraction préalable est commise à l'étranger dans de nombreux cas, les prévenus transférant ensuite les fonds en Suisse. Il n'est pas rare que ceux-ci soient par la suite virés de nouveau à l'étranger, vers le pays d'origine ou d'autres États avec des places financières importantes. Dans certains cas, les transactions sont en outre exécutées par une ou plusieurs sociétés écrans des criminels pour cacher l'identité des ayants droit économiques. Ces structures alambiquées sont plutôt utilisées pour des escroqueries vastes et complexes. Par ailleurs, les actifs sont aussi retirés en espèces puis expédiés à l'étranger via des établissements de transfert de fonds pour interrompre la piste de l'argent. Ce mode opératoire a été observé en particulier en relation avec des agents financiers. Souvent, les escrocs ont également utilisé les fonds dérobés pour financer leur style de vie dispendieux ou pour rembourser des dettes. Dans le cas d'infractions telles que le *rip deal* ou le coup du neveu, l'argent volé passe la frontière en espèces principalement.

Le nombre d'infractions en concurrence réelle est lui aussi très varié. En général, plusieurs articles de loi s'appliquent lors de procédures d'envergure concernant la criminalité économique. En plus de l'escroquerie, il s'agit souvent d'abus de confiance, de gestion déloyale, d'utilisation frauduleuse d'un ordinateur et de faux dans les titres, les banqueroutes frauduleuses jouant plus rarement un rôle. La preuve d'une escroquerie étant contraignante en raison de la structure en cascade, il est fréquent que les enquêtes des autorités de poursuite pénale mettent d'abord en lumière d'autres infractions. Pour employer aussi efficacement que possible les ressources disponibles dans une procédure, il peut être judicieux dans certains cas d'axer cette dernière sur l'infraction déjà identifiée et d'abandonner le grief d'escroquerie, à condition que la peine encourue soit identique. Il est dès lors vraisemblable qu'une partie des communications de soupçons au MROS supposant une escroquerie comme infraction préalable ait finalement débouché sur une procédure pour abus de confiance ou gestion déloyale. De manière générale, des experts en poursuite pénale estiment qu'il faudrait parler de délinquants économiques, et non d'escrocs, car cela correspond mieux au phénomène.

La pluralité des formes d'escroqueries en Suisse n'est recensée que partiellement; les différents phénomènes ne peuvent donc être analysés que dans une certaine mesure. Concernant la cybercriminalité, y compris de nombreux phénomènes d'escroquerie susmentionnés, la SPC devrait offrir de meilleures possibilités d'analyse dès l'année prochaine[110]. De même, la SUS se limite aux articles de loi concernés. Les communications de soupçons internes à fedpol (communications au MROS et sur la cybercriminalité) fournissent des possibilités d'analyse

[110] Un nouveau modèle de saisie de la cybercriminalité dans la SPC, y c. les cyber-escroqueries, devrait être disponible à partir de 2021.

plus vastes, mais elles sont peu appropriées pour évaluer l'ampleur du phénomène. Les sondages auprès des victimes pourraient apporter une aide supplémentaire, mais ils ne couvrent jusqu'à présent que des aspects partiels des infractions d'escroquerie et d'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur.

4.2.2 Caractéristiques complexes de l'escroquerie

L'escroquerie présente une certaine complexité en tant qu'infraction pénale: la limite entre un comportement punissable et non punissable s'accompagne, dans le cas de l'escroquerie, d'aléas sensibles qui se manifestent notamment au niveau de la tromperie et du dommage[111]. Par exemple, une escroquerie relève du droit pénal uniquement si elle se base sur une astuce.

Dans le cadre de leurs procédures pénales en Suisse, les autorités de poursuite pénale rencontrent parfois des difficultés dans la démonstration de l'astuce comme élément constitutif de l'escroquerie.

En effet, dans les cas de blanchiment d'argent ayant pour infraction préalable une escroquerie commise à l'étranger, il convient de démontrer qu'il y a eu astuce afin que la notion d'escroquerie soit conforme à celle prévue par le droit suisse. Or cette condition fait parfois défaut selon le droit étranger.

Dans certains cas, l'absence de démonstration de l'astuce comme élément constitutif d'un cas d'escroquerie commis à l'étranger a conduit à l'abandon des poursuites pour blanchiment d'argent, l'infraction préalable faisant défaut.

Par exemple, dans son arrêt du 24 novembre 2010 (SK.2010.9), le Tribunal pénal fédéral n'avait pas reconnu la commission d'une escroquerie comme infraction préalable à un cas de blanchiment d'argent, dans la mesure où le droit russe, soit le pays dans lequel l'escroquerie était soupçonnée d'avoir été commise, avait une acception plus large de l'escroquerie que le droit suisse et ne prévoyait pas l'astuce comme élément constitutif.

Le critère de l'astuce constitue un défi pour les autorités de poursuite pénale, même lorsque les actes sont commis en Suisse. Sans démonstration de l'astuce, il arrive régulièrement que certains cas ne peuvent pas se solder par une condamnation. On peut citer, à titre d'exemple, une procédure contre un prétendu voyant qui affirmait pouvoir prédire les chiffres du loto. Environ 700 personnes lésées lui avaient payé des émoluments de 65 francs pour obtenir ces chiffres. Le critère de l'astuce n'étant pas démontré, le ministère public compétent décida de mettre fin à la procédure. Lors de petites sommes notamment, la victime doit peser les tenants et les aboutissants d'une plainte éventuelle et d'une procédure sans savoir si ce critère sera finalement reconnu.

D'autres caractéristiques de l'escroquerie peuvent compliquer l'administration des preuves. Il est difficile de chiffrer le dommage lorsqu'il y a un grand nombre de lésés, de comptes et de transactions et lorsque les rendements dus ont été versés au moins en partie. De plus, en vertu du principe de l'identité matérielle[112], le dommage (= désavantage patrimonial) doit correspondre à l'enrichissement (= avantage patrimonial). En d'autres termes, l'enrichissement recherché par le criminel à des fins personnelles ou pour des tiers doit être le revers du dommage occasionné à la victime[113].

De même, le lien de causalité entre les éléments constitutifs d'une escroquerie peut poser problème: dans certains cas, les lésés ont effectué un acte de disposition de leur patrimoine sans qu'il y ait eu à ce stade de tromperie. Celle-ci se manifeste uniquement au moment du

---

[111] Maeder/Niggli (2009), référence susmentionnée, p. 3093.
[112] Gunther Arzt (2007): *Art. 146*, dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2e édition, Bâle, 2007, p. 551.
[113] Référence susmentionnée.

remboursement ou lorsqu'une part des rendements est exigée. Dans cette situation, les conditions objectives de l'escroquerie ne sont pas forcément remplies, car la décision qui mène à un acte de disposition du patrimoine du lésé doit être la conséquence directe d'une erreur[114].

Enfin, les jugements examinés révèlent que la preuve de l'intention (élément subjectif) constitue un défi tant pour l'escroquerie que pour le blanchiment d'argent (à l'instar d'autres domaines de la criminalité économique). Les escrocs n'appliquent pas toujours une stratégie définie à l'avance, mais agissent parfois de manière plutôt spontanée. Par conséquent, il est parfois difficile d'évaluer si une intention criminelle prévalait dès le début d'une escroquerie ou si l'auteur d'une escroquerie au placement, par exemple, a cru un moment à sa stratégie d'investissement. Cela vaut aussi pour d'éventuels complices qui, par essence, n'ont qu'un accès restreint aux informations importantes. Dans la plupart des cas, un enquêteur expérimenté peut, en vérifiant les connaissances du prévenu, déterminer le moment dans les opérations où cette personne aurait dû tirer le signal d'alarme même si elle a cru à sa stratégie. Si elle ne l'a pas fait, l'intention criminelle peut généralement être supposée.

Compte tenu de cette complexité, le résultat d'une procédure pour escroquerie est souvent plus incertain que dans d'autres infractions pénales (vol, p. ex.). Il en découle une certaine vulnérabilité, car toutes les victimes n'accepteront probablement pas le risque d'un procès lorsque seuls des petits montants sont en jeu et qu'il existe un risque de réputation.

4.2.3 Délais de prescription différents entre l'infraction préalable et le blanchiment d'argent simple

Certaines procédures pour escroquerie durent très longtemps non seulement en raison de l'entraide judiciaire internationale, mais également à cause du nombre de personnes concernées ou de la complexité générale du cas.

Dans ce contexte, l'extension du droit de participer dans le Code de procédure pénal en vigueur, qui accorde notamment à toutes les parties légitimées à faire recours le droit d'assister à l'administration des preuves par le ministère public et les tribunaux et de poser des questions aux comparants[115], représente un défi considérable sur le plan purement logistique en cas de vaste procédure pour escroquerie. De plus, et ce point revêt une importance accrue, les complices sont ainsi autorisés à assister à l'audition des autres auteurs de l'infraction. Le projet actuel de révision du CPP entend cependant restreindre ce droit de participer[116].

Les délais de prescription différents entre l'infraction préalable (15 ans pour l'escroquerie et l'utilisation frauduleuse d'un ordinateur) et le blanchiment d'argent simple (10 ans) peuvent parfois conduire à des situations dans lesquelles le jugement de première instance ne confirmera l'existence d'une infraction préalable qu'une fois le délai de prescription déjà échu pour le blanchiment d'argent. Si l'escroc et le blanchisseur sont des personnes différentes, ce dernier pourrait alors s'en tirer impunément. Ce scénario ne concerne toutefois que des cas très complexes et assez rares qui, en outre, ne relèvent pas du blanchiment d'argent qualifié.

---

[114] Référence susmentionnée, p. 540.
[115] Art. 147 CPP.
[116] Conseil fédéral (2019): pour un code de procédure pénale davantage en adéquation avec la pratique. 28 août 2019, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76205.html.

Exemple de l'affaire Behring

Le financier bâlois Dieter Behring a mis en place dès 1994 un système de placement reposant prétendument sur une solution informatique qu'il avait développée pour identifier le «code génétique de la bourse». En réalité, seule une infime partie des avoirs des clients était placée, les rendements étant généralement modestes, voire négatifs. Dieter Behring utilisait les apports des nouveaux clients pour verser les produits du capital déjà investi et s'enrichir personnellement. Ce système de répartition (également appelé système de Ponzi) basé sur plus de 800 millions de francs s'est effondré à l'automne 2004. En juin de la même année, le MROS avait informé le MPC de mouvements suspects sur des comptes en lien avec Behring. Peu après, le MPC a ouvert une enquête de police judiciaire contre Behring et contre inconnu. La procédure pénale de première instance a duré douze ans: le 30 septembre 2016, le Tribunal pénal fédéral a condamné Behring à une peine privative de liberté de cinq ans et six mois pour escroquerie par métier au détriment d'environ 2'000 lésés. Le 7 août 2018, le Tribunal fédéral a confirmé le jugement de première instance sur le plan pénal. La procédure concernant le blanchiment d'argent a pris fin en raison de la prescription. Le Tribunal a rejeté les actes de blanchiment d'argent qualifié, dont le délai de souscription est plus long, car le caractère professionnel ne s'appliquait qu'à l'infraction préalable et non au blanchiment d'argent subséquent. Dieter Behring est décédé au printemps 2019.

4.2.4 Preuve de l'infraction préalable

Non seulement la preuve de l'infraction préalable pose problème lorsqu'elle est apportée sur le plan judiciaire après la prescription de l'acte subséquent de blanchiment d'argent, mais elle constitue également une difficulté en cas d'escroquerie ou d'utilisation frauduleuse d'un ordinateur commises à l'étranger, notamment. Même en Suisse, il est parfois difficile de déduire à partir d'une transaction financière suspecte quelle est l'infraction préalable en question – nécessaire pour caractériser l'infraction pénale de blanchiment d'argent. Au demeurant, dans les procédures examinées pour le présent rapport, la plupart des classements étaient dus à l'impossibilité de prouver l'infraction préalable dont étaient issues les valeurs patrimoniales[117]. Dans d'autres cas, le tribunal a conclu qu'il n'y avait aucun acte d'entrave. Par exemple, un versement sur son propre compte bancaire en Suisse ne saurait, en général, être assimilé à un tel acte[118].

4.2.5 Différences de procédure en matière de blanchiment d'argent et d'escroquerie

Les procédures déclenchées par une communication de soupçons de blanchiment d'argent ayant une escroquerie comme infraction préalable présumée ne sont que partiellement comparables à celles qui sont initiées en premier lieu à cause d'une escroquerie. Dans le premier cas de figure, ces procédures concernent souvent une infraction d'escroquerie commise à l'étranger. Dans de tels cas, les fonds arrivent ensuite en Suisse d'une manière ou d'une autre et la place financière helvétique est vraisemblablement utilisée aux fins de blanchiment d'argent. La plupart du temps, des articles de presse ou des bases de données spécialisées attirent l'attention des intermédiaires financiers suisses sur l'implication d'un client dans un tel crime, de sorte que ceux-ci effectuent alors un signalement au MROS. Les autorités de poursuite pénale compétentes tentent par la suite de déterminer si les actifs déposés en Suisse proviennent effectivement de ce crime.

Il est toutefois fréquent que les procédures relatives à une escroquerie, en particulier au niveau cantonal, ne soient pas engagées en raison d'une communication de soupçons de blanchiment d'argent, mais pour d'autres motifs. Souvent, les autorités de poursuite pénale agissent sur plainte des lésés. Les autorités fédérales de poursuite pénale, en particulier, ouvrent aussi régulièrement des procédures sur la base de demandes d'entraide judiciaire venant d'autres

[117] Office fédéral de la police fedpol (2014), référence susmentionnée.

[118] Cf. ATF 124 IV 274, consid. 4., p. 279 et 280.

pays. Si des transactions vers l'étranger ou d'autres actes d'entrave sont découverts à la suite d'enquêtes pour escroquerie, les enquêteurs les documentent en vue d'une mise en accusation pour blanchiment d'argent. Par ailleurs, l'identification d'actes de blanchiment d'argent dans des procédures pour escroquerie n'a qu'une priorité subalterne, car une condamnation supplémentaire pour blanchiment d'argent n'augmenterait la peine que de manière marginale, de sorte que les investigations contraignantes en la matière ne se justifient pas du point de vue économique de la procédure. Il est donc probable qu'un grand nombre d'actes de blanchiment d'argent ayant des infractions d'escroquerie comme infraction préalable ne fassent l'objet d'aucune enquête et ne soient pas recensés. Cela devrait également être le cas dans d'autres domaines: lors de trafics de stupéfiants ou de vols, les enquêtes ne sont pas étendues systématiquement au blanchiment d'argent, car le travail correspondant à fournir ne se justifie pas dans la plupart des cas. Contrairement aux conséquences pénales, l'identification d'actes de blanchiment d'argent revêt une grande importance en matière de protection ou de confiscation des actifs. En examinant en détail les transactions, les retraits d'espèces, les investissements et d'autres actes d'entrave, les enquêteurs peuvent comprendre où les actifs obtenus frauduleusement ont été transférés. Idéalement, ceux-ci sont ensuite bloqués, puis confisqués à la fin de la procédure.

4.2.6 Confiscation des actifs en temps opportun

Dans certains cas, les escroqueries rapportent des millions à leurs auteurs. Ces actifs sont confisqués par les tribunaux selon le principe qui veut que le crime ne paie pas. Cette confiscation constitue toutefois un défi. Dans l'idéal, les recherches détaillées sur les actifs disponibles dans l'entourage de l'auteur doivent être réalisées à un stade précoce de la procédure. Elles peuvent cependant retarder la procédure proprement dite et ne sont dès lors pas toujours engagées systématiquement à ce moment précis. En outre, le recensement et l'examen méticuleux des prétentions des lésés sont très contraignants et mobilisent beaucoup de ressources. Par ailleurs, les enquêteurs sont souvent confrontés à une structure frauduleuse opaque au début de la procédure, les flux financiers ne pouvant fréquemment être compris qu'au bout de plusieurs mois ou années d'enquête. Les substituts, qui découlent par exemple du mélange d'actifs légaux et illicites, compliquent encore davantage la confiscation. De plus, les escrocs attribuent typiquement la faute de l'effondrement du système à la police et aux autorités de poursuite pénale et assurent que les rendements auraient été payés prochainement si la police et le ministère public n'étaient pas intervenus. Compte tenu de la colère et de l'incompréhension vis-à-vis des autorités de poursuite pénale, peu de lésés s'adressent à la police, privant celle-ci d'informations importantes. Il n'est pas rare que les lésés se montrent également peu coopératifs parce qu'ils ont investi des valeurs patrimoniales non déclarées aux autorités fiscales[119].

4.2.7 Non-identification d'une infraction pénale

Les autorités de poursuite pénale sont tenues, dans les limites de leurs compétences, d'ouvrir et de conduire une procédure lorsqu'elles ont connaissance d'infractions ou d'indices permettant de présumer l'existence d'infractions[120]. Le fait que certaines escroqueries passent fréquemment inaperçues, en particulier celles qui concernent les marchandises et les denrées alimentaires ainsi que, ponctuellement, lors d'autres phénomènes, peut alors s'avérer problématique. Le client final qui achète une huile d'olive frelatée intentionnellement, mais vendue comme extra-vierge, ne remarquera probablement jamais qu'il a été escroqué. L'auteur n'a donc guère besoin de procéder à des actes complexes pour blanchir l'argent ainsi obtenu, étant donné que l'infraction préalable n'a pas été décelée. Cela ne signifie pas pour autant que ces actifs ne sont pas blanchis. Au contraire: eu égard aux nombreuses escroqueries

[119] Office fédéral de la police fedpol (2011a): rapport annuel 2010, p. 18. https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2010-f.pdf.
[120] Art. 7 CPP.

présumées dans le secteur alimentaire, le blanchiment devrait porter sur des montants considérables. Ces actes de blanchiment ne seront toutefois pas découverts, car les fonds semblent apparemment licites. Le fait que certains types d'escroquerie restent inaperçus entraîne donc une vulnérabilité majeure.

5 Évaluation du risque lié à l'escroquerie et à l'utilisation frauduleuse d'un ordinateur comme infractions préalables au blanchiment d'argent

5.1 Conséquences pour la Suisse

Les conséquences des infractions d'escroquerie en tant qu'infractions préalables au blanchiment d'argent sont difficiles à estimer, mais un système efficace de défense et de lutte semble globalement éviter qu'elles n'influent sur la société, le secteur financier ou le secteur tertiaire. Les dommages financiers peuvent certes être considérables pour les différentes victimes ou pour l'État (p. ex. en cas d'escroquerie au placement), mais les possibilités de confiscation des actifs et les créances compensatrices les atténuent au moins partiellement. La législation relative au blanchiment d'argent peut également avoir un effet préventif, car elle permet de bloquer certains paiements suspects.

5.2 Évaluation finale du risque de blanchiment d'argent

La menace inhérente aux infractions d'escroquerie et d'hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur en tant qu'infractions préalables au blanchiment d'argent n'a pas vraiment changé ces dernières années. Son évolution dans un avenir proche dépendra essentiellement de celle de la cybercriminalité. Les données actuelles sont néanmoins encore trop insuffisantes pour réaliser une prévision précise. Celle-ci nécessiterait d'autres études scientifiques, notamment des sondages auprès des victimes axés sur ces infractions. Dans des cas individuels, les escroqueries peuvent avoir des conséquences financières ou psychiques majeures. Jusqu'à présent, l'ampleur et l'impact de ces infractions pénales ne posent, dans l'ensemble, aucun risque d'importance systémique pour la Suisse, comme en témoigne le montant relativement modeste du crime dans la plupart des cas (en général, moins de 10'000 francs). Le rapport révèle cependant que certaines escroqueries peuvent être de grande ampleur et avoir de vastes conséquences dans des circonstances particulières. Dans de tels cas, la principale menace vient toutefois principalement de l'infraction préalable, et pas nécessairement de l'acte subséquent de blanchiment d'argent. Le risque que la place financière suisse soit abusée pour blanchir des actifs provenant d'escroqueries commises à l'étranger, où elles peuvent présenter une importance systémique, semble plus probable.

En théorie, les utilisations frauduleuses d'un ordinateur et les escroqueries sont presque toujours suivies d'un ou de plusieurs actes de blanchiment d'argent, à condition qu'elles ne soient pas considérées comme des infractions d'importance mineure contre le patrimoine. Il convient de supposer que la plupart des criminels ne se contentent pas d'accumuler l'argent sur leur propre compte, mais l'utilisent également d'une manière qui peut être assimilée au blanchiment d'argent. Les technologies de l'information et de la communication offrent certes de nouvelles possibilités d'escroquerie qui s'accompagnent en partie d'un transfert présumé de la criminalité dite classique vers la cybercriminalité, mais le risque de blanchiment d'argent n'a pas vraiment changé ces dernières années. Tout comme les infractions préalables d'escroquerie et d'utilisation frauduleuse d'un ordinateur, ce risque ne présente pas d'importance systémique.

Les autorités de poursuite pénale mettent toutefois davantage l'accent sur les actes de blanchiment d'argent et la cybercriminalité. La plupart du temps, les infractions d'escroquerie commises grâce à Internet nécessitent des transferts d'argent via des intermédiaires financiers. Un système de contrôle efficace permet souvent d'identifier le caractère illégal de ces transac-

tions. Le principal risque de blanchiment d'argent se pose lorsque les actifs à blanchir ne peuvent pas être identifiés, suivis et confisqués à temps. En particulier, les très nombreux cas dans lesquels des montants relativement faibles sont blanchis depuis ou à l'étranger posent problème. Il n'est pas rare qu'ils s'appuient sur des agents financiers. Les petites transactions sont souvent plus difficiles à détecter, car elles ne sortent pas vraiment de l'ordinaire. De plus, lorsqu'elles sont découvertes, elles engendrent un travail relativement important pour l'autorité de poursuite pénale chargée de l'enquête. Par conséquent, les principaux risques de blanchiment d'argent devraient provenir des formes d'escroquerie qui sont réalisées la plupart du temps grâce à Internet: i) escroquerie sur des sites de vente en ligne et des portails immobiliers, ii) hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur, iii) escroqueries au placement et iv) faux ordres de virements internationaux. Les v) escroqueries liées à la faillite d'entreprise et la vi) fraude alimentaire présentent elles aussi des risques. Les deux premiers phénomènes recèlent un risque accru de blanchiment d'argent, notamment en raison de leur ampleur et du montant total des dommages. Certes relativement faibles, de nombreux montants sont ainsi blanchis en Suisse ou à l'étranger. Les escroqueries au placement et les faux ordres de virement sont quant à eux porteurs de risques en raison des conséquences financières généralement importantes pour les personnes concernées et donc des actifs élevés à blanchir. Les escroqueries liées à la faillite d'entreprise n'étaient pas l'objet principal du présent rapport en raison des infractions particulières connexes. Beaucoup d'éléments, dont le niveau élevé des dommages estimés, indiquent cependant que ces infractions présentent elles aussi un risque de blanchiment d'argent pour la Suisse. Enfin, il convient de mentionner la fraude alimentaire qui, d'après plusieurs indicateurs, est de grande ampleur. Cette dernière est généralement sous-estimée, car la fraude n'est pas identifiée la plupart du temps. En outre, la fraude alimentaire est l'une des rares formes d'escroquerie qui pose également un risque sanitaire dans le pire des cas.

L'évaluation des risques des différents phénomènes d'escroquerie est résumée dans le tableau ci-après:

Évaluation des risques		
Menace *(threat)*	Vulnérabilité *(vulnerability)*	Conséquences *(consequences)*
Escroquerie lors de faillites d'entreprises	· Vérification déficiente des liquidités par les créanciers lors de leasings et de commandes · Jusqu'à présent, procédure peu systématique en matière de prévention et de répression · Manque de sensibilisation des services concernés (office des faillites, notaires, etc.)	· Dommages financiers considérables (notamment pour la collectivité)
Fraude à la TVA de type carrousel	· Difficile à détecter · Difficilement identifiable en tant qu'escroquerie	· Dommages élevés pour la collectivité
Fraude aux marchés publics	· Difficile à détecter	· Dommages élevés pour la collectivité
Hameçonnage	· Envoi de masse · Faible investissement technique pour obtenir les données · Criminels à l'étranger · Entraide judiciaire pas toujours simple	· Perte de confiance dans les échanges commerciaux en ligne · Souvent, impossibilité de condamner les criminels

	▪ Infractions très complexes sur le plan technique	
Faux ordres de virements internationaux	▪ Infrastructure informatique peu protégée ▪ Système de contrôle interne rudimentaire ▪ Criminels à l'étranger ▪ Entraide judiciaire pas toujours simple ▪ Utilisation présumée de systèmes de virement informels	▪ Dommages financiers élevés pour les entrepreneurs ▪ Souvent, impossibilité de condamner les criminels
Escroquerie au crédit	▪ Faibles charges de travail pour les criminels ▪ Procédure souvent standardisée pour l'octroi de crédits	▪ Dommages élevés pour les prêteurs
Escroquerie à l'assurance	▪ Procédure souvent standardisée pour la déclaration de sinistres	▪ Dommages financiers très variables
Fraude alimentaire	▪ N'est souvent pas détectée ▪ Chaînes d'approvisionnement complexes avec de nombreux acteurs ▪ Ramification internationale fréquente	▪ Dommages financiers très variables ▪ Risque pour la santé dans les cas extrêmes
Escroquerie sur les sites de vente en ligne et les portails immobiliers	▪ Faible investissement technique ▪ Interruption du *paper trail* ▪ Petits montants ▪ Utilisation disproportionnée des ressources pour les enquêtes	▪ Souvent, une victime avec un dommage financier faible uniquement ▪ Perte de confiance vis-à-vis du négociant ▪ Répétitivité élevée
Escroquerie au placement	▪ Faits et «produits» complexes ▪ Vérifications parfois difficiles pour les investisseurs ▪ Vaste procédure avec de nombreux lésés	▪ Perte de confiance dans les placements ▪ Dommages très élevés pour les investisseurs
Fausse demande de soutien	▪ Criminels à l'étranger qui utilisent de fausses identités ▪ Entraide judiciaire pas simple ▪ Aucun *paper trail* en cas de numéraire	▪ Victimes renonçant à porter plainte, car elles ont honte ▪ Arrestation des seuls collecteurs de fonds; commanditaire souvent pas condamné
Prestation d'aide trompeuse	▪ Criminels à l'étranger qui utilisent de fausses identités ▪ En général, aucun *paper trail*, car il s'agit souvent de numéraire	▪ Parfois, dommages financiers élevés pour les particuliers ▪ Arrestation des seuls collecteurs de fonds; commanditaire souvent pas condamné
Escroquerie à l'avance de frais	▪ Envoi de masse ▪ Interruption du *paper trail* ▪ Petits montants ▪ Criminels à l'étranger qui utilisent de fausses identités	▪ Souvent, une victime avec un dommage financier relativement faible ▪ Parfois, endettement auprès de l'entourage social

	▪ Entraide judiciaire pas toujours simple	▪ Risque de dépendance psychique vis-à-vis des criminels ▪ Souvent, impossibilité de condamner les criminels
Escroquerie au change	▪ En général, aucun *paper trail*, car il s'agit souvent d'opérations en numéraire	▪ Dommage élevé en cas de *rip deal* ▪ Souvent, dommages relativement faibles pour les autres variantes
Escroquerie au mariage / *romance scam*	▪ Exploitation de la solitude des victimes ▪ Criminels à l'étranger qui utilisent de fausses identités ▪ Entraide judiciaire pas toujours simple	▪ Dommages financiers très variables ▪ Dommages psychiques pour les victimes ▪ Souvent, impossibilité de condamner les criminels
Escroquerie au prêt	▪ Petits montants	▪ Souvent, une victime avec un dommage financier relativement faible
Obtention ou vente frauduleuse de marchandises	▪ N'est parfois pas détectée ▪ Ramification internationale fréquente	▪ Dommages financiers très variables

5.3 Recommandations

Les constatations effectuées dans ce rapport se traduisent par les recommandations suivantes à l'attention du GCBF:

- **Améliorer l'évaluation de la situation:** ce rapport révèle que les données actuelles ne recensent que partiellement les infractions d'escroquerie et d'hameçonnage à des fins d'utilisation frauduleuse d'un ordinateur. Même si la complexité de l'escroquerie et, dans une moindre mesure, de l'utilisation frauduleuse d'un ordinateur ne pourra jamais être appréhendée intégralement, des améliorations restent possibles. Des sondages indépendants et réguliers auprès des victimes, reposant sur une base scientifique, portant spécifiquement sur les infractions d'escroqueries et d'hameçonnages et englobant les personnes tant morales que physiques, contribueraient à une meilleure vue d'ensemble. Concernant les statistiques existantes, en particulier la SPC, il faudrait évaluer dans quelle mesure il est possible de mieux saisir statistiquement la pluralité des formes d'escroqueries[121]. Il serait notamment envisageable que les escroqueries réalisées hors ligne soient systématiquement ventilées selon leur forme dans la SPC[122]. Il conviendrait également d'évaluer si et dans quelle mesure le montant du dommage et l'infraction préalable pourraient être recensés pour les infractions de blanchiment d'argent.

[121] Un nouveau modèle de saisie de la cybercriminalité dans la SPC, qui s'appuie notamment sur le catalogue des phénomènes établi par fedpol, devrait être disponible en 2021 pour les données de l'année 2020.
[122] P. ex. à l'aide des catégories d'escroquerie en vigueur: escroquerie (non spécifiée), escroquerie au prêt, escroquerie au crédit, escroquerie à l'avance, escroquerie au change, obtention/vente frauduleuse de marchandise, obtention/vente frauduleuse de véhicule, escroquerie à l'assurance, escroquerie au mariage, escroquerie au chèque, escroquerie au jeu et escroquerie d'hôtel.

- **Poursuivre la sensibilisation:** la Suisse dispose déjà de mécanismes de prévention professionnels qui sont bien développés (cf. point 1.2). Toutefois, les escrocs trouvent constamment de nouveaux moyens de tromper les victimes. Il est donc essentiel que les acteurs de la prévention soient informés continuellement des modes opératoires les plus récents et adaptent et complètent régulièrement leurs conseils à la population. Concernant la cybercriminalité, la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 prévoit d'ores et déjà une «détection précoce des tendances ou technologies et l'acquisition des connaissances utiles» ainsi qu'une sensibilisation accrue[123]. Le renforcement de la sensibilisation devrait également être examiné pour les formes d'escroquerie réalisées hors ligne.

[123] Conseil fédéral (2018): stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022. https://www.isb.admin.ch/dam/isb/fr/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf.

6 Bibliographie

Ackermann, Jürg-Beat (2019): Das Submissionskartell – Sicht des Strafrechts. Lucerne 18.02.2019.
https://www.unilu.ch/fileadmin/fakultaeten/rf/diebold/Tagung_Submissionskartell/Ackermann_Submissionskartell_Strafrecht.pdf [04.03.2020]

Arzt, Gunther (2007): *Art. 146*, dans: Niggli, Marcel Alexander / Wiprächtiger, Hans (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2e édition, 2007, pp. 513-558

Balzli, Tina (2018): *Art. 3 Abs. 1 lit. r*, dans: Heizmann, Reto / Loacker, Leander D. (éditeur): UWG Bundesgesetz gegen den unlauteren Wettbewerb. Kommentar. Zurich 2018 pp. 700-726

Beaudet-Labrecque, Olivier / Brunoni, Luca / Augsburger-Bucheli, Isabelle (2018a): Abus financiers. Étude nationale concernant les abus financiers commis à l'encontre des personnes de 55 ans et plus. Pro Senectute Suisse (éditeur). Zurich 2018.
https://www.prosenectute.ch/dam/jcr:e0a731a4-ab86-4810-b10c-e4f532374ad4/Finanzieller-Missbrauch-Studienbericht-01.10.2018.pdf [04.03.2020]

Beaudet-Labrecque, Olivier / Brunoni, Luca / Augsburger-Bucheli, Isabelle (2018b): «Abus financiers» - les abus financiers les plus fréquents en Suisse. Pro Senectute Suisse (éditeur). Zurich 2018.
https://www.prosenectute.ch/dam/jcr:7d5c59ff-5b6b-468c-8666-3a6d21abe729/Finanzieller-Missbrauch-haeufigste-Betrugsformen-in-der-Schweiz-01.10.2018.pdf [04.03.2020]

Biberstein, Lorenz / Killias, Martin / Walser, Severin / Iadanza, Sandro / Pfammatter, Andrea (2016): Sondage au sujet des expériences et opinions sur la criminalité en Suisse. Analyses dans le cadre du sondage national de sécurité 2015

Brunner, Alexander (2007): *Art. 163*, dans: Niggli, Marcel Alexander / Wiprächtiger, Hans (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 2e édition, Bâle 2007, pp. 785-797

Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2019): OPSON VIII: Vérification de l'étiquetage du café. 06.2019.
https://www.newsd.admin.ch/newsd/message/attachments/57404.pdf [04.03.2020]

Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2018a): OPSON VII: a-t-on coloré le thon pour le rendre plus appétissant? 04.2018.
https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-eu-opson-thunfisch.pdf.download.pdf/Schlussbericht_OPSON_VII_FR.pdf [04.03.2020]

Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2018b): rapport annuel 2017 sur les programmes de contrôle à la frontière. Surveillance des denrées alimentaires végétales et des objets usuels.
https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/bericht-grenzkontrollen-2017.pdf.download.pdf/Jahresbericht_Kontrollprogramme_an_der_Grenze_2017_zu_pflanzl._LM_und_GG_FR.pdf [04.03.2020]

Office fédéral de la sécurité alimentaire et des affaires vétérinaires (2016): campagne nationale de détection des pratiques frauduleuses dans la commercialisation des miels et des poissons.
https://www.blv.admin.ch/dam/blv/fr/dokumente/lebensmittel-und-ernaehrung/lebensmittelsicherheit/verantwortlichkeiten/zusammenfassung-bericht-nat-kontrollprogramm-betrug-honig-fisch.pdf.download.pdf/Rapport_pour_le_public,_campagne_authenticit%C3%A9_miels_et_poissons,_R%C3%A9sum%C3%A9_F_2.pdf [04.03.2020]

Office fédéral de la police fedpol (2020): les différentes formes d'escroquerie
https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/gefahren/betrugsarten.html [04.03.2020]

Office fédéral de la police fedpol (2018): dangers liés à Internet
https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/gefahren.html
[04.03.2020]

Office fédéral de la police fedpol (2015): rapport annuel 2014 du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI),
https://www.fedpol.admin.ch/dam/data/fedpol/cybercrime/Berichte/2015-03-26/jb-kobik-f.pdf
[04.03.2020]

Office fédéral de la police fedpol (2014): jugements prononcés en Suisse en matière de blanchiment d'argent.
https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/geldwaeschereiurteile_okt2014-f.pdf [04.03.2020]

Office fédéral de la police fedpol (2011a): Rapport annuel 2010. Lutte de la Confédération contre la criminalité.
https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2010-f.pdf [04.03.2020]

Office fédéral de la police fedpol (2011b): Agents financiers: le blanchiment d'argent comme activité accessoire lucrative (non publié)

Office fédéral de la statistique (2019a): Statistique des condamnations pénales.
https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/justice-penale.html
[04.03.2020]

Office fédéral de la statistique (2019b): Statistique policière de la criminalité.
https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police.html
[04.03.2020]

Office fédéral de la statistique (2019c): Nouvelle augmentation du nombre d'ouvertures de faillites. Version du 11.04.2019.
https://www.bfs.admin.ch/bfsstatic/dam/assets/7966849/master

Office fédéral de la statistique (2019d): Statistique policière de la criminalité (SPC). Rapport annuel 2018 des infractions enregistrées par la police.
https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal/police.assetdetail.7726192.html [04.03.2020]

Office fédéral de la statistique (2017): Statistique policière de la criminalité (SPC). Aide à la saisie SPC V06.00. 01.01.2017.
https://www.bfs.admin.ch/bfsstatic/dam/assets/2103674/master [04.03.2020]

Ministère public de la Confédération (2019): manipulations des émissions polluantes des véhicules du groupe VW: questionnaire en ligne pour les lésés. Communiqué de presse du 2 septembre 2019, https://www.bundesanwaltschaft.ch/mpc/fr/home/medien/archiv-medienmitteilungen/news-seite.msg-id-76267.html [04.03.2020]

Ministère public de la Confédération (2014): la Suisse indemnise les lésés dans l'affaire Allen Stanford, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-52261.html [04.03.2020]

Conseil fédéral (2019): Pour un code de procédure pénale davantage en adéquation avec la pratique. 28.08.2019. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76205.html. [04.03.2020]

Conseil fédéral (2018): Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). 2018 à 2022. https://www.isb.admin.ch/dam/isb/fr/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf [04.03.2020]

Conseil fédéral (2013): message du 13 décembre 2013 concernant la mise en œuvre des recommandations du Groupe d'action financière (GAFI), révisées en 2012, FF *2014* 585. https://www.admin.ch/opc/fr/federal-gazette/2014/585.pdf [04.03.2020]

Conseil fédéral (2011): message du 25 mai 2010 relatif à la loi fédérale sur les denrées alimentaires et les objets usuels, FF *2011* 5181. https://www.admin.ch/opc/fr/federal-gazette/2011/5181.pdf [04.03.2020]

Conseil fédéral (2009): message du 2 septembre 2009 concernant la modification de la loi fédérale contre la concurrence déloyale (LCD), FF *2009* 5539. https://www.admin.ch/opc/fr/federal-gazette/2009/5539.pdf [04.03.2020]

Conseil fédéral (1991): message du 24 avril 1991 concernant la modification du code pénal suisse et du code pénal militaire (infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (dispositions pénales), FF *1991* II 933. https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10106593 [04.03.2020]

Chainalysis (2019): *Crypto Crime Report. Decoding Hacks, Darknet Markets, and Scams*. https://blog.chainalysis.com/ [04.03.2020]

Der Bund (2016): *Der Check als Auslaufmodell*. 23.06.2016. https://www.derbund.ch/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/wirtschaft/geld/der-check-als-auslaufmodell/story/17304703 [04.03.2020]

Egmont Group of Financial Intelligence Units (2019): *Business Email Compromise Fraud*, dans: Egmont Group Bulletin. https://www.egmontgroup.org/sites/default/files/filedepot/external/20190708_EGMONT%20GROUP%20BEC%20BULLETIN-final.pdf [04.03.2020]

EUROPOL (2019): *228 arrests and over 3800 money mules identified in global action against money laundering*. Communiqué du 04.12.2019.
https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering [04.03.2020]

EUROPOL (2016): *EUROPOL strengthens efforts to tackle social engineering*. Communiqué du 28.01.2016.
https://www.europol.europa.eu/latest_news/europol-strengthens-efforts-tackle-social-engineering [04.03.2020]

Commisison européenne (2018): *Knowledge Centre for Food Fraud and Quality. Infographic.* https://ec.europa.eu/knowledge4policy/sites/know4pol/files/a0infographic_kc_food_fraud_final_0.pdf [04.03.2020]

Fiolka, Gerhard (2019): *Art. 147*, dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111–392 StGB. Basler Kommentar, 4e édition, Bâle, 2019, p. 3173

Galli, Peter / Moser, André / Lang, Elisabeth / Steiner Marc (2013): *Praxis des öffentlichen Beschaffungsrechts. Eine systematische Darstellung der Rechtsprechung des Bundes und der Kantone*. 3e édition. Zurich 2013

Groupe d'action financière GAFI (2013): *National Money Laundering and Terrorist Financing Risk Assessment. FATF Guidance*, février 2013.
www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf [04.03.2020]

Groupe d'action financière GAFI (2012): *Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération.* The FATF Recommandations. Actualisé en juin 2019.
https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Recommandations%20du%20GAFI%202012.pdf [04.03.2020]

Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme, GCBF (2018a): rapport sur l'utilisation du numéraire et les risques inhérents d'utilisation abusive pour le blanchiment d'argent et le financement du terrorisme en Suisse, octobre 2018
https://www.newsd.admin.ch/newsd/message/attachments/55178.pdf [04.03.2020]

Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme, GCBF (2018b): rapport sur le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding, octobre 2018
https://www.newsd.admin.ch/newsd/message/attachments/55112.pdf [04.03.2020]

Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme, GCBF (2017): Risque de blanchiment d'argent associé aux personnes morales, novembre 2017.
https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-nov-2017-f.pdf [04.03.2020]

Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme, GCBF (2017): Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, juin 2015.
https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-juni-2015-d.pdf [04.03.2020]

Groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme, GCBF (2015b): communiqué de presse concernant le rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse, juin 2015.
https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-57750.html [04.03.2020]

Levi, Michael (2008): *Organized fraud and organizing frauds. Unpacking research on networks and organization*, dans: Criminology and Criminal Justice, Vol 8 (49), pp. 389-419. https://www.researchgate.net/profile/Michael_Levi4/publication/249786379_Organized_fraud_and_organizing_fraudsUnpacking_research_on_networks_and_organization/links/0c960532755df02414000000/Organized-fraud-and-organizing-fraudsUnpacking-research-on-networks-and-organization.pdf [04.03.2020]

Maeder, Stefan/ Niggli, Marcel Alexander (2019): *Art. 146* dans: Marcel Alexander Niggli / Hans Wiprächtiger (éditeur): Strafrecht II, Art. 111-392 StGB. Basler Kommentar, 2e édition, Bâle, 2019, pp. 3084-3159

NTV (2012): *Handel mit Falsch-Käse entlarvt*. 17.06.2012.
https://www.n-tv.de/panorama/Handel-mit-Falsch-Kaese-entlarvt-article6750746.html [04.03.2020]

PricewaterhouseCoopers (2018): *Gesunken, aber nicht geschlagen: Schweizer Wirtschaftskriminelle werden digital und suchen sich neue Tätigkeitsfelder*. *Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse*.
https://www.pwc.ch/de/publications/2018/globale-umfrage-zur-wirtschaftskriminalitaet-2018.pdf [04.03.2020]

RTS (2013): Du cheval à la place de bœuf dans des tartares servis en Suisse.
https://www.rts.ch/info/suisse/5329304-du-cheval-a-la-place-de-boeuf-dans-des-tartares-servis-en-suisse-.html [04.03.2020]

Sakic, Senad (2015): *Gewerbsmässige Firmenbestattung. Masterarbeit am Competence Center Forensik und Wirtschaftskriminalität*. Haute école de Lucerne, Lucerne 2015

Association suisse d'assurances ASA (2017): Escroquerie à l'assurance : chiffres et faits. Résumé des résultats de l'étude GfK sur la fraude à l'assurance. 31.08.2017.
https://www.svv.ch/sites/default/files/2017-11/ASA%20résumé%20des%20résultats%20de%20l%27étude%20GFK%20sur%20la%20fraude%20à%20l%27assurance%202017.pdf [04.03.2020]

SRF (2016): *Konkursreiterei: Mehrere Hundert Millionen Schaden im Jahr*. 13.04.2016.
https://www.srf.ch/news/schweiz/konkursreiterei-mehrere-hundert-millionen-schaden-im-jahr [04.03.2020]

Trechsel, Stefan / Crameri, Dean (2012): *Art. 146 Betrug*, dans: Stefan Trechsel / Mark Pieth (éditeur): Schweizerisches Strafgesetzbuch Praxiskommentar, 2e édition, Zurich 2012, pp. 736-766

Weissenberger, Philippe (2019): *Art. 172ter*, dans: Niggli, Marcel Alexander / Wiprächtiger, Hans (éditeur): Strafrecht II, Art. 111-392 StGB. Basler Kommentar, 4e édition, Bâle 2019, pp. 3550-3563

Arrêts du Tribunal fédéral:

ATF 116 IV 343. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F116-IV-343%3Ade&lang=de&type=show_document [04.03.2020]

ATF 126 IV 165. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F126-IV-165%3Ade [04.03.2020]

ATF 129 IV 315. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F129-IV-315%3Ade [04.03.2020]

ATF 134 IV 210. http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F134-IV-210%3Ade [04.03.2020]

ATF 124 IV 274. http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F124-IV-274%3Ade&lang=de&type=show_document [04.03.2020]

ATF 1A.189/2001 du 22.02.2002. www.polyreg.ch/bgeunpub/Jahr_2001/Entscheide_1A_2001/1A.189__2001.html [04.03.2020]

ATF 6P.172/2000 und 6S.776/2000 du 14.5.2001. www.polyreg.ch/bgeunpub/Jahr_2000/Entscheide_6P_2000/6P.172__2000.html [04.03.2020]

Arrêt du Tribunal pénal fédéral:

Arrêt du Tribunal pénal fédéral SK.2010.9 du 24.11.2010. https://bstger.weblaw.ch/cache/pub/cache.faces?file=20101124_SK_2010_9.htm&ul=fr [04.03.2020]