www.jusletter-it.eu

Fabian Teichmann / Léonard Gerber

La surveillance informatique

Un outil efficace contre le financement du terrorisme à l'exemple des crypto-monnaies

Cette contribution illustre l'aptitude des crypto-monnaies au financement du terrorisme, après une présentation du cadre juridique suisse en matière de répression pénale, de compliance et des développements récents en matière de tokens. Les auteurs étudient parallèlement l'opportunité de l'introduction d'une nouvelle mesure de surveillance informatique pouvant contribuer à enrayer les formes modernes du financement du terrorisme.

Catégories d'articles : Blockchain
Région : Switzerland
Domaines juridiques : Blockchain

Proposition de citation : Fabian Teichmann / Léonard Gerber, La surveillance informatique, in : Jusletter IT 12 novembre 2020

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Table des matières

Introduction

[1] Les autorités de poursuite pénale et les instituts financiers comme les banques ont la responsabilité de mener une lutte efficace contre le blanchiment d'argent et le financement du terrorisme. Cette approche de la répression du financement du terrorisme suggérée par le Groupe d'Action Financière (GAFI) suite aux attentats du 11 septembre 2001[1] part du principe que combiner la répression pénale individuelle des criminels avec la responsabilisation des instituts financiers chargés de paralyser les sources de financement des terroristes garantit une lutte plus efficace contre le terrorisme.[2] Or, l'innovation technologique financière moderne comme les crypto-monnaies et leur émission par Initial Coin Offerings (ICO) renforcent une tendance à la désintermédiation financière, plus spécialement des banques qui ne sont plus à la source des transactions et du financement.[3] De plus, l'anonymat offert par les transactions liées aux crypto-monnaies offre aux terroristes un moyen de financer leurs activités sans passer par des contrôles de compliance.[4] Après une brève présentation de comment la Suisse implémente les standards internationaux de lutte contre le financement du terrorisme au niveau légal (I), la présente contribution analyse les risques de financement du terrorisme liés aux crypto-monnaies et la réponse actuelle des autorités suisses (II). Enfin, les auteurs considèrent la possibilité d'introduire la surveillance informatique comme nouvelle mesure de contrainte du CPPSuisse en vue de lutter contre le financement du terrorisme (III).

1 Rapport annuel du GAFI 2001–2002, daté du 2 juin 2002, p. 1.

2 Voir l'annexe A du Rapport annuel 2001–2002 du GAFI, « Eight Special Recommendations on Terrorist Financing ». D'autres stratégies existent comme des mesures de sécurité de l'aviation civile (Detlof Von Winterfeldt/Terrence O'Sullivan, « Should we protect commercial airplanes against surface-to-air missile attacks by terrorists ? », Decision Analysis, 3(2), p. 63–75, p. 63) la conduite de guerre conventionnelle (Jules Lobel, « The use of force to respond to terrorist attacks : The bombing of Sudan and Afghanistan », Yale Journal of International Law, vol. 24, p. 537s, Ruth Wegdwood, « Responding to terrorism : The strikes against Bin Laden », Yale Journal of International Law, vol. 24, p. 559–576, p. 559s.), la restriction de la mobilité des terroristes (Ersel Aydinly, « From finances to transnational mobility : Searching for the global jihadist's achilles heels », Terrorism and Political Violence, vol. 18 (2), p. 301–313, p. 301s.).

3 Pour un article détaillé voir Marco Dell'Erba, « Initial Coin Offerings – The first response of regulatory authorities », NYU Journal of Law & Business 2018, Vol. 14, p. 1109–1137, p. 1119.

4 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9 ; Voir également Jana Drzalic/Giovanni Molo, Können Krypto-Währungen compliant sein ?, AJP 2019, p. 40–57, p. 41.

I. Législation suisse contre le financement du terrorisme

[2] Au niveau international, la définition du financement du terrorisme n'a pas encore trouvé de consensus.[5] La Convention internationale pour la répression du financement du terrorisme du 9 décembre 1999[6] encourage les États à prendre les mesures nécessaires pour incriminer pénalement le financement du terrorisme. Elle sert dans beaucoup de pays comme base pour l'implémentation de normes anti-terrorisme au niveau domestique. En parallèle, le GAFI, un organisme international, émet des recommandations aux États pour implémenter des mesures de prévention et de répression du financement du terrorisme, du blanchiment d'argent et du crime organisé.[7] Les États signataires sont libres d'incorporer ces recommandations au niveau de leur législation interne de manière contraignante.

[3] La Suisse s'est conformée à la Convention internationale ainsi qu'aux recommandations du GAFI en incriminant le financement du terrorisme et le blanchiment d'argent au niveau pénal fédéral.[8] Ainsi, celui qui se rend coupable de financement du terrorisme est passible de 5 ans de peine privative de liberté au plus ou d'une peine pécuniaire.[9] S'agissant du volet de la prévention, la loi fédérale sur le blanchiment d'argent (LBA)[10] confie la responsabilité de la lutte contre le financement du terrorisme, du blanchiment d'argent et du crime organisé notamment aux intermédiaires financiers.[11] Les devoirs découlant de cette responsabilité prévus par la LBA sont exhaustifs et l'OBA[12], l'OBA-FINMA[13], les règlements des organismes d'autorégulation (art. 25 LBA) ainsi que la convention relative sur l'obligation de diligence des banques (CDB)[14] en concrétisent la portée.[15]

[4] Les intermédiaires financiers doivent ainsi prévoir des procédures de compliance adéquates pour s'assurer que les transactions effectuées par leurs biais ne sont pas liées à des activités terroristes.[16] À cet égard, ils ont un devoir d'identification de l'ayant-droit économique, et de vérification de l'objet et du but de la relation d'affaires souhaitée par chaque cocontractant sur la base

---

5 Cooper Helen, « Terrorism : the problem of definition revisited », American Behavioral Scientist 2001, vol. 44 No. 6, p. 881–893, p. 881 ; Ruby Charles, « The definition of terrorism », Analyses of Social Issues and Public Policy *2002*, vol. 2, No. 1, p. 9–14, p. 9f. ; Tilly Charles, « Terror, terrorism, terrorists », Sociological Theory 2004, vol. 22 No. 1, p. 5–13, p. 5f. ; Tofangsaz Hamed, « A new approach to the criminalization of terrorist financing and its compatibility with Sharia law » Journal of Money Laundering Control 2012, p. 386–406, p. 386.

6 Entrée en vigueur pour la Suisse au 23 octobre 2003 (RS 0.353.22).

7 Alexander Kern, « The international anti-money-laundering regime : The role of the Financial Action Task Force », 2001, Journal of Money Laundering Control, vol. 4 No. 3, p. 231–248, p. 231.

8 Ce dispositif se base d'une part sur l'art. 260^{quinquies} CP et d'autre part sur la loi sur le blanchiment d'argent, ci-après LBA (RS 955.0). Voir à cet égard, Guillaume Grisel, « Le trust en Suisse », LaPD 2020, p. 269–283, p. 269.

9 CP art. 260^{quinquies}.

10 RS 955.0.

11 Urs Zulauf/Doris Hutzler, « Der begründete und der einfache Verdacht », recht 4/2019, p. 221–239, p. 222.

12 Ordonnance sur le blanchiment d'argent du 11 novembre 2015 (RS 955.01).

13 Ordonnance de l'Autorité fédérale de surveillance des marchés financiers sur la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier du 3 juin 2015 (RS 955.033.0).

14 Une version électronique est disponible sur : https ://www.swissbanking.org/fr/medias/positions-et-communiques-de-presse/convention-relative-a-l2019obligation-de-diligence-des-banques-cdb-revisee-entree-en-vigueur-debut-2016 (09 juillet 2019).

15 Peter Nobel, Internationales und nationales Wirtschaftsrecht, insbesondere Wettbewerbs- und Kartellrecht/ Wirtschaftsrecht und wirtschaftliche Betrachtungsweise, dans : Grolimund/Koller/Loacker/Portmann (Ed.) Festschrift für Anton K. Schnyder zum 65. Geburtstag, Zurich 2018, p. 1217–1239, p. 1228s.

16 Nobel, p. 1227ss.

de pièces justificatives.[17] Si des indices laissent supposer un cas de financement du terrorisme, l'intermédiaire financiers doit clarifier l'arrière-plan et le but de la transaction ou de la relation d'affaires.[18] Cette obligation de diligence concrétise ainsi les « know your customer rules » et a pour objectif la transparence et la prise en compte des risques liés au financement du terrorisme et au blanchiment d'argent ainsi que la détermination des personnes et entités avec lesquelles l'intermédiaire financier entre en relation.[19]

[5] Toutefois, les moyens de clarification à disposition des intermédiaires financiers pour déterminer l'arrière-plan des transactions et des relations d'affaires de leurs cocontractants sont difficilement adéquats.[20] Par exemple, la prise de renseignement[21] auprès des cocontractants, des détenteurs de contrôle ou des ayants-droit économiques se basent sur les pièces justificatives de leurs clients qui sont largement susceptibles de manipulation ou d'abus, voire de faux dans les titres.[22] Ils peuvent également effectuer une visite des lieux où ces derniers conduisent leurs affaires, également susceptibles de manipulation.[23] En réalité, ces moyens ne doivent pas faire des intermédiaires financiers comme les banques des substituts des autorités de poursuite pénale chargées de l'enquête et de la collecte des preuves mais simplement de vérifier s'il existe des soupçons justifiant une communication au Bureau de communication en matière de blanchiment d'argent (MROS).[24] En effet, la LBA consacre une obligation de communication auprès du MROS lorsque des soupçons fondés se présentent pour l'intermédiaire financier que des valeurs patrimoniales sont liées au financement du terrorisme.[25] Sur la base de la communication, le MROS effectuera la dénonciation auprès de l'autorité de poursuite pénale compétente après vérification des soupçons de l'intermédiaire financier.[26]

II. L'aptitude des crypto-monnaies au financement du terrorisme

[6] Malgré ces systèmes préventifs et répressifs, le financement du terrorisme demeure toujours un problème global[27] parce que différentes méthodes s'offrent encore aux terroristes pour finan-

17 Voir les art. 3, 4, 6 et 7 LBA.

18 Voir plus particulièrement l'art. 6 LBA.

19 Favrod-Coune Pascal, *Crowdfunding – Analyse de droit Suisse du financement participative* CEDIDAC, Lausanne 2018, p. 566–584, p. 575, voir également André Tanner, « Der bankinterne Compliance Officer », Jusletter 30 septembre 2019, p. 4.

20 Friedrich Schneider, « Money laundering and financial means of organised crime : Some preliminary empirical findings », Global Business and Economics Review 2008, Vol. 10 No. 3, p. 309–330 p. 309s.

21 OBA-FINMA art. 16 I let. a.

22 Voir par exemple, Fabian Teichmann/Léonard Gerber, « Tendances du blanchiment d'argent et du financement du terrorisme », Jusletter 18 novembre 2019, p. 7ss. Pour une analyse détaillée, voir le rapport du Egmont Group of Financial Intelligence Units « FIU's in Action : 100 Cases from the Egmont Group », disponible sous le lien suivant : https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei/jb.html (24 juin 2020).

23 *Idem* ; OBA-FINMA art. 16 I let. b.

24 Voir à cet égard le Message concernant la modification du code pénal suisse et du code pénal militaire du 30 juin 1993, FF 1993 III 269, p. 317 ainsi que Hutzler/Zulauf, p. 223.

25 Voir l'art. 9 LBA. Pour la notion de « soupçons fondés » voir Hutzler/Zulauf, p. 222.

26 Voir l'art. 23 LBA.

27 Voir à cet égard Jackie Harvey, « Compliance and reporting issues arising for financial institutions from money laundering regulations : A preliminary cost benefit study », Journal of Money Laundering Control 2004, p. 333–346, p. 339, Petrus Van Duyne, « Money Laundering : Estimates in Fog », Journal of Financial Crime 1994, vol. 2 No. 1, p. 58–74, p. 62 ; John Walker, « How big is global money laundering ? », Journal of Money Laundering 1999, p. 25–37, p. 36.

cer leurs activités à l'écart des procédures de compliance strictes.[28] Le GAFI attire notamment l'attention des États sur les risques émanant des valeurs virtuelles et des prestations de service liées aux valeurs virtuelles[29] Il encourage ainsi les États à soumettre les prestataires de services liés aux valeurs virtuelles à une licence ou à une obligation d'enregistrement.[30] Les prestations visées concernent nommément l'échange, le transfert, la gestion et l'administration de valeurs virtuelles ou d'instruments assurant le contrôle de ces valeurs virtuelles ainsi que la participation et les provisions des prestations financières liées à l'offre et/ou la vente de valeurs virtuelles.[31]

[7] Plus concrètement, les transactions liées aux crypto-monnaies posent un problème de transparence aux autorités régulatrices et aux autorités de poursuite pénale.[32] D'une part, les crypto-monnaies peuvent être négociées sur internet, garantissant l'anonymat des parties et leur permettant d'effectuer des virements anonymes sans passer par un intermédiaire financier soumis à l'obligation de diligence.[33] D'autre part, les transactions par voie de crypto-monnaies peuvent impliquer des infrastructures complexes dans plusieurs pays, impliquant différentes autorités de surveillance et différents standards de compliance en matière de lutte contre le financement du terrorisme.[34] Il existe donc un risque de conflits de compétence des autorités et de standards différents en matière de compliance et d'entraide judiciaire internationale.[35] De plus, les émetteurs peuvent eux-mêmes procéder à l'émission de leurs jetons (ICO) sans devoir faire auditer les documents des projets qu'ils fournissent aux potentiels investisseurs.[36] Le risque principal est que l'émetteur utilise les fonds pour financer des actes de terrorisme ou que des sommes d'origine criminelle soient investies dans une ICO.[37] Bien que les systèmes de paiement soient assujettis à la LBA[38], le GAFI relève toutefois que le niveau d'anonymat offert par les systèmes de crypto-monnaies sur internet est sans comparaison avec les systèmes de paiements traditionnels.[39] À cet égard, les plateformes de négociation de crypto-monnaies ne sont pas assujetties à la LBA lorsqu'elles n'exercent ni une activité nécessitant une licence bancaire ni une activité d'intermédiation financière, plus particulièrement lorsqu'elles ne font que relier les acheteurs et les vendeurs sans intervenir dans les transactions de leurs clients.[40]

---

28 Voir le rapport du Egmont Group of Financial Intelligence Units « FIU's in Action : 100 Cases from the Egmont Group », disponible sous le lien suivant : https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei/jb.html (24 juin 2020). Voir également Teichmann/Gerber, p. 8ss.

29 FATF, Guidance for a risk-based approach to virtual assets and virtual asset service providers, p. 55.

30 FATF, Guidance for a risk-based approach to virtual assets and virtual asset service providers, p. 55.

31 FATF, Guidance for a risk-based approach to virtual assets and virtual asset service providers, p. 13s.

32 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9, voir également Drzalic/Molo, p. 41.

33 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9 ; Rapport du groupe interdépartemental de coordination sur la lute contre le blanchiment d'argent et le financement du terrorisme (GCBF) publié en octobre 2018, « le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding », p. 32

34 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9 ; Rapport du GCBF, p. 32.

35 Rapport du GCBF, p. 35.

36 S'agissant des documents nécessaires à une ICO voir Dell'Erba, p. 1115. Voir également Roger Aitken, Investment Guide to « Crypto » Coin Offerings Rating Blockchain Start-ups, Forbes 6 janvier 2017, disponible sous le llien suivant : https ://www.forbes.com/sites/rogeraitken/2017/01/06/investment-guide-to-crypto-coin-offerings-rating-blockchain-startups/#68cdadf6121b (28 août 2020)

37 Pour une étude détaillée, voir le Rapport du GCBF, p. 37ss.

38 Voir l'art. 2 II let. d^{ter} LBA.

39 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9s.

40 Pour une étude détaillée voir Drzalic/Molo, p. 41. Voir également le Rapport du GCBF, p. 34

[8] Au-delà des risques de fraude en lien avec l'ICO, d'évaluation du cours et d'insolvabilité de l'émetteur, l'identité des parties et des ayants-droit économiques ainsi que la provenance des fonds pourront rester cachées à défaut de passer par un intermédiaire financier et d'un contrôle de compliance adéquat.[41] Cet anonymat profite non seulement aux terroristes eux-mêmes mais également aux personnes souhaitant financer ces activités terroristes. Il implique des risques réduits que les transactions fassent l'objet d'une procédure pénale.[42] Les transactions liées aux crypto-monnaies font partie d'une tendance actuelle générale à la désintermédiation financière[43] de sorte que les transactions effectuées par les terroristes ne doivent plus nécessairement passer par un intermédiaire financier soumis à l'obligation de diligence. Ces transactions peuvent se faire par des plateformes liant directement les investisseurs aux émetteurs, comme les plateformes de e-trading, par l'appel aux donations de la part des adhérents, voire par des banquiers hawalas.[44] Ainsi, les bitcoins permettent par exemple d'effectuer des transactions anonymes sur le *darkweb*, servant aux terroristes pour acheter du matériel, des explosifs, des armes ou recevoir des donations.[45]

[9] Cependant, les crypto-monnaies ne permettent pas aux terroristes de financer les charges de la vie quotidienne.[46] Par exemple, un terroriste vivant à Berlin, à Vienne ou à Zurich ne pourra pas payer ses courses avec des bitcoins. Lorsque les terroristes nécessitent de financer leurs activités quotidiennes en vue de la préparation d'attaques, ils auront donc besoin d'échanger leurs bitcoins contre des euros ou des francs suisses par exemple. En raison de leur anonymat, les crypto-monnaies peuvent toutefois être utiles comme moyen de paiement pour acheter des armes ou des explosifs pour une future attaque terroriste. En conclusion intermédiaire, les crypto-monnaies ont en général une grande aptitude au financement du terrorisme.

[10] En réponse à cette situation, la FINMA a publié un guide pratique sur les ICO en février 2018 ainsi qu'un complément datant du 11 septembre 2019.[47] Le guide pratique traite des questions d'assujettissement notamment au système préventif du blanchiment d'argent et de financement du terrorisme, des types de jetons qu'elle traitera en tant que valeurs mobilières et de l'applicabilité de la loi sur les banques, la loi sur les placements collectifs et la loi sur les établissements financiers pouvant impliquer un assujettissement à la surveillance de la FINMA. Concrètement, la FINMA différencie trois types de jetons, à savoir les jetons de paiement, les jetons d'utilité et les jetons d'investissement.[48] De plus, le complément précise la notion de *stablecoins* et l'applicabilité de la LB, la LPCC, la LBA, la LSFin et de la LIMF, faisant régulièrement l'objet de requêtes ten-

41 FINMA, Communication sur le traitement prudential des initial coin offerings datée du 29 septembre 2017, p. 4 ; FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9 ; Drzalic/Molo, p. 49ss. ; Dell'Erba, p. 1114ss.

42 FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 9s.

43 Dell'Erba, p. 1119.

44 Dell'Erba, p. 1119 ; Drzalic/Molo, p. 41 ; FATF 2013, « The role of Hawala and other similar service providers in money laundering and terrorist financing », p. 16 (https://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf).

45 Voir par exemple le cas de Silk Road traité dans FATF, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, 2014, p. 11.

46 Voir Fabian Teichmann « Financing Terrorism through Cryptocurrencies – A Danger for Europe ? », Journal of Money Laundering Control 2018, Vol. 21, N°4, p. 513–519, p. 518.

47 Tarek Houdrouge/Jérémie Tenot, « Le droit suisse à l'heure de la technologie des registres électroniques distribués », Not@lex 2020, p. 49–63, p. 51.

48 FINMA, Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO), 16 février 2018.

dant à une décision de non-assujettissement de la FINMA.[49] La FINMA se base sur ces distinctions pour déterminer si les jetons en question doivent être qualifiés en tant que valeurs mobilières[50], ainsi que de droits-valeurs[51] et établir le cas échéant une décision de non-assujettissement.[52]

[11] Enfin, le Conseil fédéral a formulé un message daté du 27 novembre 2019 relatif au projet de loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués.[53] Cette loi d'adaptation prévoit de modifier une dizaine de lois fédérales notamment en créant une nouvelle autorisation dans le droit des infrastructures des marchés financiers pour les systèmes de négociation fondés sur la technologie des registres électroniques distribués.[54] Ainsi, la Suisse compte se conformer aux recommandations du GAFI en intégrant les plateformes de négociation de crypto-monnaies au cercle des intermédiaires financiers assujettis aux règles de la LBA. L'Assemblée fédérale a adopté cette loi fédérale le 25 septembre 2020 à l'unanimité dont la période de consultation court jusqu'au 2 février 2021 et l'entrée en vigueur prévue au 1er août 2021.[55]

III. La surveillance informatique comme outil de lutte contre le financement du terrorisme

[12] À défaut de procédure de compliance applicable, les transactions par crypto-monnaies susceptibles d'être liées à un financement du terrorisme ne seront premièrement pas détectées par un intermédiaire et ne feront ainsi pas l'objet d'une communication au MROS ni d'une procédure pénale le cas échéant. En outre, des modes d'opération des terroristes compliquent la collecte de preuves et d'indices par les autorités de poursuite pénale. La surveillance informatique pourrait remédier en partie à ce problème (ci-après A). Une réforme législative du CPP dans cette direction se heurterait cependant à des obstacles constitutionnels, notamment quant à la protection de la sphère privée. En tout cas, le pouvoir d'ordonner la surveillance informatique des autorités de poursuite pénale doit être encadré par des conditions strictes (B). Enfin, des problèmes liés à la compétence et l'entraide internationale compliquent la lutte contre le financement du terrorisme (C).

A. Efficacité de la surveillance informatique

[13] À défaut de contrôle de compliance permettant de filtrer les transactions susceptibles d'être liées au terrorisme, les autorités de poursuite pénale ont peu de ressources pour constater les faits et collecter des preuves à charge (resp. à décharge). À cet égard, l'internet joue un grand

49 Houdrouge/Tenot, p. 51.

50 Art. 2 let. b LIMF et art. 3 let. b LSFin.

51 Voir l'art. 973c III CO.

52 Voir à cet égard Houdrouge/Tenot, p. 51.

53 Voir Message relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués du 27 novembre 2019, FF 2020 223, p. 223.

54 Voir FF 2020 223, p. 260.

55 Ordonnance du Conseil fédéral sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués – Rapport explicatif du DFF en vue de l'ouverture de la procédure de consultation daté du 19 octobre 2020.

rôle dans l'organisation du terrorisme. Les organisations terroristes y ont recours pour diffuser de la propagande, organiser des attentats, ou simplement échanger des informations techniques.[56] Les terroristes l'utilisent pour communiquer par le biais d'emails, de forums de discussion, de chats de news et services de messagerie.[57] Les terroristes et sympathisants y trouvent également une importante source d'information pouvant favoriser la radicalisation ou le recrutement de nouveaux adhérents et collecter des fonds.[58] La surveillance informatique est particulièrement pertinente s'agissant des personnes planifiant des activités terroristes de manière isolée, communément appelées « lonely wolves ».[59] Internet offre une source d'information à ces personnes qui peuvent également se radicaliser et acheter du matériel comme une camionnette ou des armes par ce biais par exemple en utilisant des crypto-monnaies.[60]

[14] Plus particulièrement s'agissant des infractions liées aux crypto-monnaies, le rapport du GCBF relève lui-même les limites du système préventif actuel du financement du terrorisme en lien avec les crypto-monnaies.[61] Les autorités de poursuite pénale ne parviennent pas à percer l'anonymat lié aux transactions en crypto-monnaies et aux portfolios les accompagnant.[62] Cette situation résulte en la prononciation de nombreuses ordonnances de non-entrée en matière de la part des ministères publics lorsqu'ils reçoivent des dossiers du MROS.[63] Les procédures d'enquête se voient confrontées à l'impossibilité d'identifier l'ayant-droit économique des portfolios de crypto-monnaies dont l'origine est suspecte.[64] L'entraide internationale s'avère toujours un instrument important de la répression de la criminalité liée aux crypto-monnaies.[65]

[15] La surveillance informatique permet à l'investigateur de pénétrer dans l'ordinateur de l'inculpé par un programme internet de type *GovWare* ou cheval de Troie sans passer par les fournisseurs de services de télécommunication.[66] L'investigateur en atteignant l'ordinateur de l'inculpé à son insu pourra surveiller ses activités sans l'inquiéter.[67] Cette méthode s'avère plus efficace que l'observation. De plus les découvertes sont plus facilement documentées par la surveillance informatique que par l'infiltration par agent, ce dernier devant subséquemment offrir son témoignage.[68] Ainsi, les informations consignées par surveillance sont contenues dans un support de données sous une forme écrite. Il s'agit également d'une façon plus simple de surveiller des conversations téléphoniques effectuées par internet.[69]

---

56 Mara Todeschini, Terrorismusbekämpfung im Strafrecht, Zürich 2019, p. 4.

57 Todeschini, p. 4.

58 Michael Lauber/Alexander Medved, *Kriminalität, Strafrecht, und Föderalismus*, Bern 2019, p. 194.

59 Teichmann, p. 516.

60 Teichmann, p. 516.

61 Rapport du GCBF, p. 35.

62 Rapport du GCBF, p. 35.

63 Rapport du GCBF, p. 35.

64 Rapport du GCBF, p. 35.

65 Voir notamment l'exemple de Silk Road 2 dont le serveur physique du site web criminel a pu être perquisitionné en Suisse sur la base d'une requête d'entraide judiciaire, dans Rapport du GCBF, p. 41.

66 Sylvain Métille, Mesures techniques de surveillance et respect des droits fondamentaux, p. 222. Pour la notion de GovWare voir Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, p. 2466.

67 Métille, p. 222.

68 Voir l'art. 269^{quater} CPP.

69 Métille, p. 148.

[16] Bien que la configuration sur mesure de la surveillance informatique s'avère particulièrement onéreuse, elle permet d'adapter les méthodes de surveillance à l'évolution technique.[70] L'engagement efficace et cible d'un *GovWare* nécessite en règle générale au préalable l'exécution d'une surveillance de la correspondance par télécommunication dite classique, au sens de l'art. 269 CPP, ainsi qu'une analyse de l'environnement social de la personne cible, pour déterminer si le support du prévenu est effectivement l'utilisateur de l'appareil cible en question (en particulier lorsque plusieurs personnes partagent la même connexion Internet dans le but d'éviter de surveiller la correspondance par télécommunication d'une autre personne que la personne cible).[71] La présence physique de l'inculpé n'est pas requise contrairement à la perquisition.[72] Un investigateur pourra surveiller à distance une multitude d'activités et d'inculpés. Du temps précieux est ainsi gagné, ce qui s'avère pertinent en considérant la pression du faible temps à disposition des autorités notamment en cas de transfert de fonds à l'étranger.

B. Vers une réforme législative

[17] Une multitude d'obstacles juridiques s'opposent à l'introduction d'une nouvelle mesure de contrainte telle que la surveillance informatique proposée ici. Ceux-ci sont d'ordre constitutionnel et concerne notamment la protection de la sphère privée. De plus, des conditions strictes doivent encadrer le pouvoir d'ordonner des autorités de poursuite pénale notamment en ce qui concerne les *fishing expedition*, les découvertes fortuites ou la garantie du secret professionnel.

1. Obstacles constitutionnels

[18] La surveillance informatique constitue une ingérence dans la sphère privée des justiciables et de la liberté personnelle.[73] Le justiciable a notamment une prétention contre l'État au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'il établit par la poste et les télécommunications.[74] Il en va spécialement de même s'agissant de l'emploi abusif de ses données.[75] Toutefois, les libertés fondamentales peuvent faire l'objet de restrictions en vertu de l'art. 36 Cst.féd. pour autant qu'elles soient prévues par loi, relèvent d'un intérêt public, soient proportionnées au but poursuivi et ne portent pas atteinte au noyau du droit fondamental.[76]

[19] En qualité de liberté fondamentale une ingérence de la part des autorités de poursuite pénale contre la sphère privée requiert une base légale.[77] Une ingérence grave requiert une base légale formelle.[78] Or, plus le domaine privé est touché, plus forte sera l'ingérence dans la sphère intime

70 Voir FF 2013 2379, p. 2469s.

71 FF 2013 2379, p. 2469.

72 Voir l'art. 245 II CPP.

73 Giovanni Biaggini, BV-Kommentar, Zurich 2017, 2ème éd., art. 13 N 10a.

74 Art. 13 Cst.féd.

75 Art. 13 II Cst.féd.

76 Biaggini, BV-Kommentar, art. 36 N 1.

77 Biaggini, BV-Kommentar, art. 13 N 10a.

78 Biaggini, BV-Kommentar, art. 36 N 13.

et privée du justiciable.[79] En considérant que la sphère privée voire même intime du justiciable soit « mise à nue » par la surveillance informatique, notamment de ses conversations, photos, contacts, qu'il ne partagerait qu'avec un cercle intime de personnes proches, il est légitime de considérer la surveillance informatique comme une ingérence grave contre le droit à la protection de la vie privé. Une telle mesure requiert donc une base légale formelle au même titre que les autres mesures de surveillance électronique prévues par le CPP.[80]

[20] La lutte contre le financement du terrorisme vise un intérêt public relevant de la répression du terrorisme, de son financement, de la sécurité publique, de la collaboration internationale et le soutien à la lutte contre le crime organisé.[81] Elle contribue également à renforcer la réputation de la place financière suisse.[82]

[21] De plus, les trois maximes du principe de la proportionnalité doivent être respectées.[83] En comparaison des autres mesures de surveillance électronique existantes, la surveillance informatique apparaît comme la mesure la plus contraignante et invasive de la sphère privée de la personne surveillée, si bien qu'elle ne devrait servir qu'en tant qu'*ultima ratio*. On ne peut toutefois exclure que la surveillance informatique puisse être ordonnée pour la poursuite d'autres infractions. Il ne faut toutefois pas perdre de vue le potentiel d'utilisation abusive de cette mesure de contrainte, dont le but ne doit pas aller au-delà de l'investigation de l'infraction du financement du terrorisme. Elle ne doit pas être utilisée abusivement par les autorités notamment en matière de *fishing expedition*.[84] Les autorités pourraient en effet être tentées d'y recourir pour sonder des infractions fiscales, sous prétexte de poursuivre un cas de financement du terrorisme. L'infraction de financement du terrorisme sauvegarde un bien juridiquement protégé supérieur à l'infraction de fraude fiscale bien que les valeurs litigieuses soient liées.[85] Les preuves obtenues d'une telle façon sont inexploitables.[86] Il devrait en aller de même des découvertes fortuites concernant des tiers non-suspectés de financement du terrorisme ou d'infractions sortant du champ d'application de la mesure, lors de la surveillance informatique du suspect.[87]

[22] Les autorités chargées de la surveillance électronique devront également respecter la protection de la bonne foi du justiciable et ne pas agir de manière arbitraire.[88] Dans l'idéal, une règlementation claire encadre les conditions nécessaires pour ordonner la surveillance électronique ainsi que son exercice par l'autorité compétente évitant qu'elle ne soit exercée arbitrairement ou au-delà du but assigné. On relèvera cependant qu'une surveillance efficace nécessite que l'inves-

---

79 Notons également que les infractions contre le domaine secret ainsi que le domaine privé, notamment l'écoute et l'enregistrement de conversations sont réprimées par les art. 179bis–179^{quater} CP.

80 Métille, p. 149.

81 Voir Message relatif aux Conventions internationales pour la répression du financement du terrorisme et pour la répression des attentats terroristes à l'explosif ainsi qu'à la modification du code pénal et à l'adaptation d'autres lois fédérales, FF 2002 5014, p. 5014ss.

82 Peter Kunz, *Wirtschaftsrecht – Grundlagen und Beobachtungen*, Zürich 2019, p. 185.

83 Art. 197 CPP repris par l'art, 269 CPP. Voir également l'ATF 141 IV 77, c. 5. (trad. JdT 2016 IV 6, c. 5.)

84 Voir notamment Jonas Weber, Kommentar Strafprozessordnung/Jugendstrafprozessordnung, ad art. 196 N 14ss.

85 Plus encore, les banques se montrent généralement très coopératrices à l'égard des autorités de poursuite pénale en matière de financement du terrorisme tout en renvoyant au secret bancaire s'agissant de la fraude fiscale. Les banques encourent des risques bien plus grand pour sauvegarder leur réputation s'agissant du financement du terrorisme, si bien qu'on parle d'une restriction sélective du secret bancaire.

86 Voir l'art. 141 CPP ainsi que les ATF 139 IV 128, c. 2.1. (trad. JdT 2014 IV 15), ATF 137 I 218, c. 2.3.2. (trad. JdT 2011 I 354).

87 Baptiste Viredaz/Stephan Johner, Commentaire romand Code de procédure pénale suisse, ad art. 197 N 5b.

88 Art. 9 Cst.féd. Voir également Giovanni Biaggini, BV-Kommentar, Zurich 2017, 2ème éd., art. 36 N 13.

tigateur ait accès à l'entier du contenu et puisse différencier entre les informations pertinentes et celles inutiles pour la procédure pénale, de sorte qu'il sera difficile d'établir une juste balance des intérêts.

2. Conditions de la surveillance informatique

[23] Des conditions strictes doivent encadrer le pouvoir des autorités pénales d'ordonner une surveillance informatique, au même titre que les autres mesures de surveillance électronique. Or, une mesure similaire à la surveillance informatique comme proposée par la présente contribution n'est pas expressément prévue par la LSCPT[89] ni par les art. 269ss. CPP. La surveillance électronique par l'installation de programmes informatiques sur un support du prévenu pour contrôler son utilisation par exemple de *WhatsApp*, *Telegram* ou *Viber* ainsi que l'utilisation d'*IMSI-Catcher* est permise depuis le 1er janvier 2018 (art. 269bis et 269ter CPP). L'utilisation de dispositifs techniques de surveillance (art. 280–281 CPP) peut également être ordonnée par le ministère public. Toutefois, une part de la doctrine considère que ces bases légales ne permettent pas d'ordonner la surveillance informatique d'un système.[90] Une norme permettant explicitement l'utilisation de la surveillance informatique pourrait trouver place en un article 298e CPP. Elle pourrait s'inspirer des travails avortés concernant le projet d'art. 18m de la loi sur le maintien de la sûreté intérieure du 21 mars 1997, ainsi que des art. 270bis et art. 269–281 CPP.[91]

[24] À cet égard, il serait adéquat de reprendre les conditions posées par les art. 269ss. CPP. Ainsi, des soupçons graves reposant sur des indices sérieux et concrets doivent laisser présumer qu'une infraction de financement du terrorisme ait eu lieu.[92] La gravité des soupçons est supérieure à celle requise par l'art. 197 CPP et doit atteindre celle requise pour la mise en détention provisoire.[93] Une mesure de contrainte ordonnée à l'aveugle sans soupçons graves relève d'une *fishing expedition*.[94] Les preuves obtenues d'une telle façon sont inexploitables.[95] Les autorités de poursuite pénale ne devraient pas non plus ordonner la surveillance informatique pour poursuivre en réalité des infractions sortant du champ d'application de la mesure sous prétexte de poursuivre une infraction de financement du terrorisme et sonder par exemple des infractions comme la fraude fiscale souvent liée à des valeurs issues du financement du terrorisme. Toutefois, l'infraction de financement du terrorisme sauvegarde un bien juridiquement protégé supé-

89 RS 780.1.

90 Contre une interprétation extensive des art. 269ter et 280 CPP pouvant inclure la surveillance informatique ou des GovWare voir notamment : Stefan Kühne/Serdar Günal Rütsche, « GovWare-Einsatz – nur zur Fernmeldeüberwachung oder auch zur technischen Überwachung ? », AJP 2019, p. 350–357, p. 351 ainsi que les références citées, Yvan Jeanneret/André Kuhn, *Précis de procédure pénale*, Berne 2018, 2ème éd., p. 414 ; Ciril Riss/Nicole Beranek Zanon, « Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern », Jusletter 9 juillet 2012, p. 2.

91 Avant-projet Fedpol du 31 janvier 2006 sur la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LSMI), disponible sous le lien suivant : https://www.newsd.admin.ch/newsd/message/attachments/1856.pdf (consulté le 20 juillet 2020).

92 Voir Sylvain Métille, Commentaire romand Code de procédure pénale suisse, ad art. 269 N 19, ainsi que l'ATF 142 IV 289, c. 2.2.1 et l'ATF 141 IV 87, c. 1.3.1. et 1.4.1. (trad. JdT 2015 IV 280).

93 Métille, Commentaire romand Code de procédure pénale suisse, ad art. 269 N 20 et les références citées.

94 Viredaz/Johner, CR CPP, ad art. 197 N 5b.

95 Voir l'art. 141 CPP ainsi que les ATF 139 IV 128, c. 2.1. (trad. JdT 2014 IV 15), ATF 137 I 218, c. 2.3.2. (trad. JdT 2011 I 354).

rieur à l'infraction de fraude fiscale.[96] Les découvertes fortuites concernant des infractions sortant du champ d'application de la surveillance informatique ou concernant des tiers, par exemple lorsqu'un ordinateur surveillé est partagé par des tiers, devraient également être inexploitables. L'investigateur devra distinguer les preuves et indices concernant l'inculpé et l'infraction de financement du terrorisme et celles concernant des tiers ou d'autres infractions sortant du champ de la mesure. Il devra aussi tenir compte des règles d'inexploitabilité des preuves par exemple lorsque des pièces sont soumises au secret professionnel conformément à l'art. 271 CPP.[97]

[25] Il convient de rappeler que la surveillance électronique et à plus forte raison la surveillance informatique devraient demeurer des *ultima ratio*.[98] L'ordre de surveillance devrait être écrit et spécifier le début et la fin de la surveillance, l'objet de la surveillance, l'identité de la personne à surveiller, l'infraction poursuivie, les personnes tenues au secret professionnel au sens de l'art. 271 CPP ou de l'art. 70b PPM, les informations techniques nécessaires, l'autorité ordonnant la surveillance et celle à qui les résultats sont destinés.[99] Le tribunal des mesures de contrainte compétent devrait subséquemment avaliser l'ordre de surveillance conformément aux art. 273 ss. CPP. C'est donc à titre d'exemple que les auteurs proposent la norme suivante :

« *Art. 298e CPP*
Surveillance informatique

a. *Le ministère public peut ordonner la surveillance informatique d'un système informatique si des faits ou des indices précis et récents permettent de supposer qu'un suspect l'utilise, lorsque :*

   a.a. *Le prévenu est fortement soupçonné d'avoir commis une infraction mentionnée à l'al. 2,*
   a.b. *Cette mesure se justifie au regard de la gravité de l'infraction, et*
   a.c. *Les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance.*

b. *La surveillance informatique de données peut être ordonnée pour les infractions suivantes :*

   b.a. *260*$^{\text{quinquies}}$ *CP*

c. *L'ordre de surveillance est soumis à l'autorisation du tribunal des mesures de contraintes*
d. *Les découvertes fortuites ne sont exploitables que lorsqu'elles concernent les infractions mentionnées à l'al. 2.*
e. *Au surplus, la surveillance informatique est régie par les art. 280–281* »

96 Plus encore, les banques se montrent généralement très coopératrices à l'égard des autorités de poursuite pénale en matière de financement du terrorisme tout en renvoyant au secret bancaire s'agissant de la fraude fiscale. Les banques encourent des risques bien plus grand pour sauvegarder leur réputation s'agissant du financement du terrorisme, si bien qu'on parle d'une restriction sélective du secret bancaire.

97 Jeanneret/Kuhn, p. 409s.

98 Métille, CR CPP, ad art. 269 N 50.

99 Le contenu correspond à l'art. 15 OSCPT. Voir à cet égard Métille, p. 162.

[26] Si théoriquement la voie du recours est ouverte contre la décision du ministère public conformément à l'art. 393 I lit. a CPP, le surveillé n'est pas censé avoir conscience de l'ordre de surveillance.[100] Cette voie de recours fait donc peu de sens d'autant plus que conformément à l'art. 274 CPP, la décision du ministère public doit encore être autorisée avec effet rétroactif par le tribunal des mesures de contrainte risquant d'annuler tout le produit de la surveillance.[101] Conformément à la jurisprudence du TF, le recours interjeté du surveillé devra attendre la communication du ministère public au tribunal des mesures de contrainte intervenant au plus tard à l'issue de la procédure préliminaire conformément aux art. 279 et 393 I lit. c CPP.[102]

C. Problèmes de compétence et d'entraide judiciaire internationales

[27] En raison de l'aspect transfrontalier des transferts de valeurs destinées à financer des activités terroristes, une réaction immédiate de l'autorité compétente territorialement est nécessaire.[103] Les valeurs suspectes transitent toutefois plus vite que l'assistance interétatique.[104] Or, les terroristes sont conscients de la lenteur des procédures d'assistance judiciaire si bien que le transfert de fonds à l'étranger n'apparaît pas spécialement problématique pour les criminels, notamment par le biais de crypto-monnaies.[105] Une réaction rapide des autorités requiert toutefois un accès adéquat aux informations permettant de fonder les soupçons.[106] Une solution serait une centrale de collecte et d'administration des données garantissant aux investigateurs un accès rapide aux informations pertinentes concernant l'inculpé. Les données pourraient ainsi être échangées entre la Suisse et l'étranger et accessibles aux investigateurs de chaque pays. Une coopération étroite entre les autorités de renseignement financier permettrait d'établir parallèlement un accès transfrontalier aux données en temps réel. De telles solutions nécessiteraient un ancrage au niveau législatif domestique, en raison de l'ingérence dans la sphère privée des justiciables.

[28] Cependant, quelles données devrait-on fournir aux autorités étrangères ? Les règles concernant les preuves obtenues illicitement en Suisse ne sont pas nécessairement les mêmes à l'étranger. Enfin, qu'en est-il si l'infraction n'est pas susceptible de faire l'objet d'une surveillance informatique dans un pays étranger ? En outre, des problèmes liés à la protection des données se posent. Ces questions doivent être résolues pour assurer l'efficacité de l'entraide judiciaire en matière de lutte contre le financement du terrorisme.

Conclusion

[29] Les crypto-monnaies représentent un danger pour la société en tant qu'elles attirent des terroristes ou des financeurs du terrorisme désireux d'opérer en tout anonymat. Cette situation s'insère dans la tendance générale à la désintermédiation financière liée notamment à l'innova-

100 Métille, p. 163.

101 Art. 279 III CPP, par renvoi de l'art. 281 IV CPP.

102 Arrêt du tribunal federal daté du 14 février 2003, 1P.15/2003. Pour une critique de ce système voir Métille, p. 162.

103 Rapport du GCBF, p. 35.

104 Rapport du GCBF, p. 35.

105 Teichmann, p. 516.

106 Rapport du GCBF, p. 35.

tion technologique. Celle-ci nécessite une adaptation du système de prévention et de répression en matière de financement du terrorisme et du blanchiment d'argent. Une option serait de règlementer les activités liées aux jetons, comme le recommande le GAFI et comme le fait indirectement la FINMA en incorporant les jetons au cadre administratif légal. Au niveau de la poursuite pénale, la collecte de preuves contre les personnes inculpées de financement du terrorisme pourrait se retrouver améliorée par l'introduction d'une nouvelle mesure de contrainte sous forme de surveillance informatique venant compléter la surveillance électronique par le biais de mesures techniques.

[30] Il est clair qu'une telle mesure de contrainte ne pourra pas faire sans autre l'objet d'un consensus politique, comme le symbolisent les tentatives avortées d'introduire dans la LSMI la surveillance de systèmes de traitements de données. Il n'est toutefois pas inutile de rappeler qu'une telle mesure de contrainte pourrait être conçue de façon à ne pouvoir toucher qu'une infime minorité de la population, ne pas impliquer le droit de surveiller n'importe quel ordinateur, et être sujette à des conditions strictes, et qu'elle viserait la protection de la population contre la menace terroriste.

Auteur : Fabian Teichmann, Teichmann International (Schweiz) AG

Co-auteur : Léonard Gerber, Teichmann International (Schweiz) AG