Communiqué de la CTIF concernant les risques de blanchiment et de financement du terrorisme liés à l'utilisation des monnaies virtuelles

Comme déjà indiqué dans le rapport annuel d'activités 2016 (mais aussi dans celui de 2017), la CTIF suit de près le phénomène des monnaies virtuelles et les risques liés à leur utilisation dans des opérations de blanchiment et de financement du terrorisme.

Les plateformes d'échange de monnaies virtuelles ne sont actuellement pas régulées en Belgique. En l'absence de cadre légal reconnaissant les plateformes, elles ne sont pas contrôlées, ni soumises au dispositif LBC/FT.

La CTIF ne reçoit dès lors pas de déclarations de soupçon provenant de plateformes d'échange en Belgique.

En revanche, les établissements de crédit en Belgique peuvent être alertés par des transactions atypiques pouvant être liées aux monnaies virtuelles et en informer la CTIF. Dans le cadre de la coopération internationale avec d'autres cellules de renseignement financier d'Etats qui agréent des plateformes d'échange, c'est entre autres le cas du Luxembourg, la CTIF peut aussi recevoir spontanément des informations sur des transactions suspectes en monnaies virtuelles, suite à une déclaration de soupçon effectuée par une plateforme d'échange à l'étranger. Ces informations sont ensuite traitées comme des déclarations de soupçon.

Les opérations liées aux monnaies virtuelles observées dans ces dossiers sont, dans la majorité des cas, des paiements internationaux à destination ou en provenance de ces plateformes d'échange ayant des comptes à l'étranger. A noter que de nombreuses personnes passent préalablement par un prestataire de services de paiement avant d'envoyer des fonds à destination d'une plateforme d'échange. Ces prestataires de services de paiement étant, dans certains cas, situés à l'étranger, il est dès lors plus difficile d'obtenir des informations sur l'origine/la destination des fonds. L'utilisation et, a fortiori, la superposition de ces prestataires de services de paiement entravent le travail d'investigation de la CTIF.

Les plateformes d'échange de monnaies virtuelles ne servent pas uniquement à convertir de la monnaie virtuelle en devises légales et inversement, mais sont également utilisées pour convertir des monnaies virtuelles en d'autres monnaies virtuelles présentant notamment un degré plus élevé d'anonymat, telles que monero ou dash[1].

La CTIF a eu connaissance de services d'échange de monnaies virtuelles contre de l'argent liquide (ou inversement) par des changeurs clandestins[2]. Ces services d'échange sont proposés par des fournisseurs de services en ligne, uniquement pour des gros montants et contre une commission bien plus importante que la commission habituelle sur les canaux courants des échangeurs en ligne. De source policière, il ressort qu'après un premier contact via une plateforme d'échange, renvoi est fait vers des canaux de communication sécurisés pour discuter des modalités de la transaction. Ensuite, les échanges physiques ont lieu durant de brèves rencontres avec les clients dans des lieux publics. Si l'échange de crypto monnaies « sales » contre de l'argent liquide via de tels fournisseurs de services en ligne pourrait sembler échapper à la justice, il ressort des poursuites pénales que ces services en ligne illégaux ne sont pas aussi anonymes que ces fournisseurs de services et leurs clients peuvent le croire, comme en témoigne récemment le démantèlement des marchés en ligne clandestins Alphabay et Hansa dans le cadre d'enquêtes pénales à l'étranger[3].

---

[1] Europol, 2017 Virtual Currencies Money laundering Typologies, Targeting Exchanges and other CyberGatekeepers, The Hague, 31/12/2017.

[2] De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten Anti Money Laundering Centre, augustus 2017, De Bilt.

[3] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

La CTIF a traité en 2016 et 2017 des déclarations de soupçon reçues d'établissements de crédit concernant des transactions financières suspectes ou atypiques avec des plateformes d'échange de monnaies virtuelles à l'étranger.

Les transactions dans ces déclarations présentent les caractéristiques suivantes :

- réception de nombreux transferts d'ordre de plateformes d'échange de monnaies virtuelles, suivis de retraits en espèces des fonds ;
- de nombreux versements en espèces suivis de l'achat de monnaies virtuelles sur des plateformes d'échange ;
- l'utilisation intensive de fournisseurs de services de paiements pour des opérations sur des plateformes d'échange de monnaies virtuelles ;
- l'exercice d'une activité non officielle de « traders » en monnaies virtuelles, sans que les revenus issus de ces activités ne soient déclarés aux autorités fiscales. Les opérations consistent en de nombreux transferts nationaux et internationaux d'ordre de multiples contreparties différentes et des versements en espèces suivis d'achats et de ventes de monnaies virtuelles sur des plateformes d'échange, visiblement pour le compte de tiers ;
- les transactions sur le compte bancaire ne correspondent pas avec le profil connu du client, qui n'exerce aucune activité déclarée, qui a des activités déclarées qui sont sans rapport avec les opérations suspectes, ou les transactions sont visiblement réalisées pour le compte de tiers ;
- le client travaille avec des plateformes d'échange connues pour faciliter l'échange anonyme de monnaies virtuelles contre du cash et vice-versa (LocalBitcoin par exemple).

Il est important de noter que, suivant les circonstances, la déclaration des revenus/plus-values retiré(e)s de l'achat et de la vente de monnaies virtuelles aux autorités fiscales peut être une obligation.

Les monnaies virtuelles peuvent être utilisées à des fins de blanchiment ou de financement du terrorisme mais également pour commettre des escroqueries. Les escroqueries sont la plupart en rapport avec des investissements en crypto-monnaies. Ces dossiers présentent les caractéristiques suivantes :

- des transferts justifiés par des investissements en crypto-monnaies où le client annonce des rendements visiblement trop élevés ;
- la réception sur un compte ouvert au nom d'un particulier/une société étrangère sans activité connue en Belgique de multiples transferts de fonds pour des montants importants avec des mentions faisant référence à des investissements en crypto-monnaies ;
- la réception de transferts importants de fonds suivis de transferts vers des places financières sensibles en matière de blanchiment où les fonds peuvent plus facilement disparaître.

Souvent ces dossiers apparaissent suite à des plaintes de clients pour des faits d'escroquerie aux investissements en crypto-monnaies. La FSMA publie sur son site internet une liste de sites internet suspects qui proposent des opérations frauduleuses de trading en crypto-monnaies. Le SPF Economie en coopération avec la FSMA a aussi créé un site spécifique qui peut être utilisé afin de vérifier si un site est négativement connu de leur service (http://temooiomwaartezijn.be/te-mooi-om-waar-te-zijn).

La CTIF a également participé à une étude dirigée par son homologue canadien Fintrac sur les monnaies virtuelles.

Il ressort de cette étude que le Bitcoin est la monnaie virtuelle la plus utilisée pour des activités illicites, au côté d'autres monnaies virtuelles comme Ethereum, Dogecoin et Litecoin. Dans la plupart des juridictions, le nombre de déclarations de soupçon concernant l'utilisation de bitcoins est en augmentation ces trois dernières années.

Même si la technologie Blockchain permet de retrouver et de tracer facilement des transactions en monnaies virtuelles, la traçabilité des transactions en monnaies virtuelles est un des problèmes majeurs identifié par les Cellules de Renseignements Financiers qui ont participé à ce projet. Les difficultés

rencontrées sont essentiellement liées à l'utilisation de technologies permettant de dissimuler l'identité des personnes qui utilisent ou exécutent des transactions en monnaies virtuelles. Il s'agit de technologies qui permettent de dissimuler ou rendre plus difficile l'identification d'une adresse IP ou de mixer plusieurs transactions en monnaies virtuelles.

L'absence dans de nombreuses juridictions de cadre légal réglementant les monnaies virtuelles, les plateformes d'échange de monnaies virtuelles et les fournisseurs de portefeuilles de stockage de monnaies virtuelles accroit encore les risques de blanchiment ou de financement du terrorisme. L'absence de cadre légal permet à certaines plateformes ou individus d'exercer des activités d'échange de monnaies virtuelles sans devoir demander de licence, ni avoir l'obligation d'appliquer des mesures LBC/FT.

De nombreuses juridictions constatent une augmentation significative du nombre de BTMs, des BTMs entre autres installés dans des casinos et salles de jeux. Les BTMs permettent de convertir, sans trop de formalités administratives d'identification, des espèces en monnaies virtuelles ou inversement des monnaies virtuelles en espèces. Les BTMs acceptent en général les bitcoins, mais aussi d'autres crypto-monnaies : Ethereum, Litcoin, Dash, Bitcoin Cash, Dogecoin, Zcash et Monero.

Des cas d'utilisation de BTMs par des organisations criminelles pour blanchir des fonds d'origine illicite ont été rapportés dans certaines juridictions. Une fois le cash converti en bitcoins, les bitcoins peuvent être aisément transférés dans une autre juridiction et éventuellement retirés à un BTM en espèces dans cette autre juridiction. Il n'existe pas en Belgique de cadre légal règlement l'installation et l'utilisation de ces BTMs.

Un certain nombre d'indicateurs d'opérations suspectes identifiés au niveau national ont été identifiés au niveau international :

- nombre important de virements d'ordre de tiers suivis de transferts vers des plateformes d'échange de monnaies virtuelles ;
- vente des monnaies virtuelles et retrait immédiat des fonds en espèces ;
- le client fournit des services financiers (plateforme d'échange de monnaies virtuelles) sans disposer d'un agrément à cet effet ;
- le client ne sait pas démontrer qu'il a satisfait à toutes ses obligations fiscales, alors qu'il exerce visiblement de manière régulière une activité de changeur (plateforme d'échange) de monnaies virtuelles;
- explications nébuleuses ou inconsistantes du client sur l'origine des fonds;
- absence de justifications économiques aux opérations ;
- opérations qui ne correspondent pas au profil du client ;
- montants ronds crédités sur un compte bancaire suivis de transferts vers des plateformes d'échange de monnaies virtuelles. Ce comportement peut s'expliquer par le fait que le client titulaire du compte est un intermédiaire qui blanchit des fonds d'origine criminelle en monnaies virtuelles pour le compte d'une organisation criminelle ;
- les transactions en monnaies virtuelles passent par des plateformes d'échange situées dans des juridictions où les plateformes d'échange sont pas ou peu contrôlées ;
- des transferts répétés et sans justification apparente de fonds d'ordre de sociétés qui exploitent des BTMs (conversion d'espèces en monnaies virtuelles);
- le client travaille avec des plateformes d'échange de type *over-the-counter*, qui favorisent les échanges anonymes de monnaies virtuelles entre particuliers, éventuellement contre du cash et vice-versa (LocalBitcoin par exemple) ;
- les documents présentés par le client pour justifier ses investissements en crypto-devises sont de piètre qualité, incomplets, frauduleux ou contiennent seulement un nombre limité d'informations sur la proposition d'investissement.

Enfin, il convient de mentionner les risques liés à la combinaison des pratiques de TBML avec l'utilisation des monnaies virtuelles. Ainsi, d'après le rapport de la Drug Enforcement Administration[4], de nombreuses sociétés basées en Chine qui produisent des biens manufacturés pour alimenter des dispositifs de TBML préfèrent les bitcoins. Le Bitcoin, très populaire en Chine permet en effet de mener à bien des transactions financières internationales, en court-circuitant le contrôle du gouvernement chinois.

[4] DEA. 2017 National Drug Threat assessment, p. 130. Consulté en ligne le 13/12/2017 : https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf