Tracfin : le renseignement financier cible les dérives du numérique

Tracfin, la cellule française de renseignement financier, a remis ce jeudi au ministre de l'Économie et des Finances, Michel Sapin, son rapport d'analyse des risques de blanchiment de capitaux et de financement du terrorisme. Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques émergents.

Selon le rapport, *« les risques d'escroquerie dans la finance participative (crowdfunding) sont élevés, par exemple par le détournement des paiements ou par l'élaboration de fraudes du type pyramide de Ponzi »*, surtout pour les plateformes de prêt. Quant aux plateformes de dons et de cagnottes en ligne, elles sont exposées à des risques *« importants de blanchiment de capitaux et de financement du terrorisme »*,. Certes, les fonds collectés restent limités, mais ils ont tout de même été multipliés par deux entre 2014 et 2015, observe Tracfin. **196,3 millions d'euros** ont été collectés via les plateformes de prêt l'an dernier, 50,3 millions d'euros pour l'investissement et 50,2 millions d'euros pour les dons.

Cadre européen pour le financement participatif

En France, un cadre juridique dédié au financement participatif a été mis en place en 2014. Il impose aux plateformes de prêt et d'investissement le choix d'un statut de conseiller en investissement participatif (CIP), régulé par l'Autorité des marchés financiers (AMF), ou d'intermédiaire en financement participatif (IFP), régulé par l'Autorité de contrôle prudentiel et de résolution (ACPR). Ces plateformes sont donc bien assujetties au dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (**LCB/FT**).

En revanche, la démarche restait facultative pour les plateformes de dons et les cagnottes en ligne. Mais elles seront aussi soumises à ce régime à partir de 2017, une ordonnance transposant une directive européenne dans ce domaine ayant été publiée le 2 décembre. C'est une bonne chose pour le directeur de Tracfin, Bruno Dalles, qui recommande l'adoption d'un cadre règlementaire dédié au financement participatif à l'échelle européenne. Car le cadre réglementaire national ne s'applique pas aux plateformes qui proposent, depuis l'étranger, d'effectuer des dons, prêts ou investissements.

Attention « particulière » pour les opérateurs

Le rapport de Tracfin s'intéresse aussi au paiement mobile. Lorsqu'il est adossé à une carte bancaire, celui-ci n'est pas plus (ni moins) risqué qu'un paiement classique par carte bancaire. Lorsque des micro-paiements et d'autres achats sont imputés sur la facture télécom du client, l'opacité est plus grande (l'opérateur télécom dispose d'une visibilité sur l'origine et la destination du paiement, mais pas la banque). L'exposition au risque de fraude est plus élevée encore pour le transfert d'argent de mobile à mobile (*cash transfer*). Dans ce cas, une somme en espèce est déposée dans un point de vente physique par un client contre la remise d'un code. Ce code sera adressé par SMS au bénéficiaire qui l'utilisera pour retirer cet argent dans un autre point de vente.

« Le cash transfer, développé par de nombreux opérateurs mobiles à travers le monde, présente les risques les plus importants en matière de blanchiment de capitaux et de financement du terrorisme [...] Les opérations, par définition non bancarisées, et dont le suivi est limité, peuvent être source d'opacité en permettant de transférer des espèces de façon anonyme et peu détectable au niveau national et international », déclare la cellule française de renseignement financier. Pour Tracfin, les opérateurs télécoms *« représentent aujourd'hui une part de marché non négligeable en termes de gestion des paiements, administrée selon des protocoles différents des architectures bancaires traditionnelles »*. Ils doivent, à ce titre, *« faire l'objet d'une attention particulière »*.

En France, le cadre juridique n'est pas unifié dans ce domaine. Néanmoins, la directive européenne révisée sur les services de paiement, dite **DSP2**, prévoit que les paiements imputés sur facture télécom soient soumis au dispositif LCB/FT dès que les montants dépassent 50 euros à l'unité, ou 300 euros en cumul par mois. Sa transposition en droit français doit intervenir d'ici fin 2017.

Anonymat des transactions virtuelles

Les monnaies virtuelles (Bitcoin, Ether...), la technologie **blockchain** et sa gestion décentralisée des transactions, ont le vent en poupe. Mais elles inquiètent les autorités. *« La monnaie virtuelle présente des risques élevés en matière de LCB/FT puisqu'elle sert de passerelle entre l'économie légale et l'économie souterraine et assure l'anonymisation des transactions »*, commente Tracfin. Elle favorise aussi, selon la cellule, le contournement des dispositifs de sanctions financières internationales, et présente des risques avérés d'escroqueries et de vols de données (hacking).

Dans ce contexte, Tracfin déplore *« l'absence de régulation »* et *« une traçabilité limitée des individus »* sur les plateformes d'échange de monnaies virtuelles. Selon l'organisation, ces manquements entravent *« le travail de l'investigation et favorisent l'utilisation de la technologie à des fins frauduleuses ».*

Importance du risque LCB/FT

Pour Tracfin, la montée en puissance de startups de la **FinTech** *« ouvre de vastes horizons »*, mais pose aussi *« des défis importants en matière de réglementation et de lutte contre la cyber-fraude »*. À ce titre, *« les deux intrusions dont a été victime le système de messagerie bancaire SWIFT au mois de février et de mai 2016 constituent un signal d'alerte sérieux »*, souligne l'organisation dans son rapport.

Tracfin recommande donc aux acteurs de la FinTech *« d'intégrer l'importance du risque LCB/FT et la nécessité de se rapprocher des autorités publiques »* pour partager l'analyse des risques nouveaux et les prévenir. À défaut, alerte Tracfin, *« le secteur s'expose à un risque de réputation, pouvant devenir un risque systémique en cas de détournement d'usage par les organisations criminelles ou terroristes »*.

Lire aussi :

Piratage de Swift : la faute à une mise à jour mal maîtrisée ?
Télégrammes : Le Note 7 cloué au sol ; Free banquier ? ; Crowdfunding pour les Shadow Brockers
Blockchain : Haro sur le hacker d'Ethereum