الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ع إ م

LETTRE D'INFORMATION : BON A SAVOIR (N°35)

Fraude à la carte bancaire : comment quelqu'un a usurpé mon identité

Petite séance témoignage. Rien de cyber pour une fois (à première vue). Il y a maintenant deux semaines, j'ai été victime de ma première fraude bancaire. Pas de skimming, pas de phishing, j'ai été confronté à une usurpation d'identité dans le monde « réel ». Avec comme conséquences, le vol d'une carte bancaire et des achats frauduleux. J'ai découpé cet article en deux parties pour en faciliter la lecture. Commençons par le début de l'histoire…

3615 my life

Après l'ouverture d'un nouveau compte bancaire, j'aurais dû en effet recevoir une carte bancaire. Procédure classique : un courrier avec le code confidentiel accompagné d'un bon de retrait de la carte en agence. Et là c'est le drame car je n'ai jamais reçu ce courrier. Il y a donc deux semaines, je vérifiais mes comptes sur l'application iPad de la banque. Oups… un retrait de 500 euros datant de la veille.

Problème : je n'ai jamais reçu le courrier et je ne suis donc jamais allé chercher ma carte… Je fais immédiatement opposition mais le mal est fait.

Le mardi suivant (et oui les agences bancaires sont fermées le lundi…), ma conseillère m'appelle et m'explique la situation. Une personne s'est présentée le samedi matin à l'agence pour récupérer ma carte bancaire en usurpant mon identité à l'aide d'un faux passeport à mon nom (je n'ai pas de passeport).

Pour récupérer et utiliser ma carte, l'escroc avait besoin du courrier, qui indique mon nom et mon code confidentiel, et qui est accompagné par le bon de retrait de la carte.

Mon courrier a donc été intercepté (il n'y a pas qu'Internet qui n'est pas sécurisé…).

Il a probablement dû être volé au centre de tri postal (ou alors c'est une fraude interne à la banque). Laissons la police faire son boulot. Dans tous les cas, cela reste une fraude certes classique (comme la police me l'a confirmé) mais sophistiquée dans l'approche : interception de courrier sensible, achat ou préparation d'un faux passeport et ensuite se risquer à récupérer la carte dans l'agence.

Conséquences

Mon compte s'est vidé de plusieurs milliers d'euros d'achat en magasins sur la seule journée de samedi. Évidemment tout est couvert par l'assurance : cela semble en effet l'une des seules actions prises pour la banque pour réduire (enfin transférer) les risques de fraudes bancaires… Le montant élevé de la fraude s'explique par le fait que la carte volée était une Visa Premier. Ce type de carte possède un plafond de retrait et de paiement sur 30 jours assez important… Mais ça marche aussi sur une journée. Ces cartes bancaires ressemblent finalement beaucoup à des cartes de crédit. Pouvoir dépenser plusieurs milliers d'euros à partir d'un compte vide (!!!) en une journée tout en ayant un découvert autorisé de quelques centaines d'euros paraît surréaliste.

Selon ma conseillère, les paiements par CB chez un commerçant ne sont vérifiés qu'à posteriori… Il paraîtrait impossible de procéder à quelques contrôles avant le paiement d'importantes transactions (surtout si elles se multiplient sous 24h) pour vérifier le solde du compte / découvert autorisé et déclencher potentiellement une petite alarme dans le système informatique de la banque (envoi d'un SMS pour confirmation ?)

Direction le commissariat

J'ai rapidement porté plainte le jour de l'appel de ma conseillère. Au commissariat de police, on a tout d'abord essayé de me faire déposer une simple main courante. Selon eux, la carte ne m'avait pas été volé car je ne l'avais jamais reçu (ça aurait donc été à la banque à porter plainte)… J'ai rétorqué (avec ironie) que je pouvais peut-être alors porter plainte pour usurpation d'identité.

Finalement, ils ont bien pris ma plainte pour escroquerie, en râlant sur le fait que j'aurais du aller dans un autre commissariat et sur le peu d'informations que la banque m'avait fourni (apparence de l'escroc, lieu du retrait au DAB…).

Ils m'ont même demandé d'aller chercher la seule « preuve » physique : le bon de retrait signé et touché par l'escroc. Au dernier moment, j'ai dû le ramener à la banque car la procédure policière n'était pas respectée…

Dans mon prochain billet, je vous parlerai des failles mises en évidence par rapport à ce type de fraude. L'usurpation d'identité est en effet un véritable fléau contre lequel les banques doivent lutter en faisant beaucoup plus d'efforts.

Usurpation d'identité et failles des agences bancaires

Comme promis, voici la suite de ma petite histoire. Intéressons-nous maintenant aux causes de ce type d'affaires. Bien sûr, on n'empêchera jamais toutes les fraudes mais dans le cas décrit dans mon dernier billet, je ne peux pas m'empêcher de mettre en évidence quelques failles dans le système.

Les failles des agences bancaires face à l'usurpation d'identité

La technique de fraude utilisée met en évidence deux principales failles de sécurité imputables à la banque :

Envoyer dans un même courrier simple : le code confidentiel et le bon de retrait.

Dans mon affaire, ça revient finalement à envoyer le code confidentiel et la carte bancaire ensemble. Le courrier est anonyme. Rien n'indique que c'est un courrier de la banque (mais paradoxalement ça donne un indice de l'importance du courrier…).

Pour la Visa Premier, le fond du courrier est en couleur (en doré…). Est-ce que cela a joué dans l'interception de mon courrier ? Je ne sais pas. J'aurais peut-être des réponses, un jour, avec la suite de l'enquête de police.

Pour le moment, aucune nouvelle. Pour en revenir au processus d'envoi des cartes bancaires (ou des chéquiers), il faut aussi savoir qu'il diffère selon les banques ou le type de carte. La plupart envoie les cartes de retrait par courrier simple.

D'autres envoient les chéquiers et les cartes bancaires classiques par courrier simple.

Chacun en tirera les conclusions qu'il voudra.

Le manque de contrôle d'identité. C'est ce que je considère comme une faute grave car l'agence bancaire a été très laxiste en matière de contrôle d'identité.

On pourrait penser que lors de la remise d'une carte bancaire une attention particulière est portée au contrôle de la pièce d'identité… Il semblerait que ça soit tout le contraire.

Lors de l'ouverture d'un compte bancaire, la banque demande une carte d'identité ou un passeport. La banque possède donc une copie de votre document d'identité. À quoi sert-elle quand on voit le nombre de fraudes à l'ouverture de compte avec de faux papiers ? À quoi sert-elle quand n'importe qui peut aller récupérer votre carte bancaire avec un faux passeport alors que vous avez fourni à votre banque votre carte d'identité ? À rien (semble-t-il). Aucune vérification sérieuse n'est effectuée (ils n'ont même pas dû vérifier ma date de naissance sur le faux passeport). C'est comme la signature pour les chèques. On vous demande de faire une jolie signature pour vous identifier (et pas authentifier…). Mais la banque ne s'en sert pas pour contrôler sur le bon de retrait. Ni sur les chèques, si j'en crois de nombreux témoignages de victimes de vol de chéquier.

La majorité des agences bancaires ne semble donc pas respecter leur réglementation pourtant supposée assez restrictive.

Qui plus est, pour créer une personne physique « sans existence légale » ou des sociétés fictives, les investissements sont modiques : pour quelques centaines d'euros seulement, on trouve des matrices de cartes d'identité sur Internet ainsi que des « templates » de justificatifs de domicile, voire des « kits complets » dans lesquels sont inclus documents d'identité, titres de séjour, attestations de domicile (factures d'opérateurs téléphoniques, relevés EDF-GDF), bulletins de salaire et attestations employeurs, diplômes scolaires, ainsi que relevés d'identité bancaire, relevés de compte, bordereaux de dépôt de chèque…

Le cadre réglementaire existe au travers des devoirs de diligence imposés par le Comité de Bâle. Le plus important d'entre eux est le **« Know Your Customer »** (KYC), qui a un double objectif :

- s'assurer de la validité et de l'authenticité d'un document d'identité et des pièces justificatives de domicile ;
- contrôler que la personne est bien celle qu'elle prétend être.

Cependant, il appartient à chaque agence bancaire d'appliquer ces vérifications d'usage. Malheureusement, trop souvent, les chargés de clientèle ne sont pas suffisamment formés à la détection de faux documents. Ce n'est pas leur métier : beaucoup se contentent de vérifier les pièces d'identité à partir d'une simple photocopie – rendant impossible le contrôle des sécurités passives propres aux documents présentés (filigrane et non-fluorescence notamment) –, et cela une fois l'ouverture du compte réalisée. Or il existe des systèmes qui, automatiquement et en seulement 3 secondes, indiquent si un document est conforme ou non. 15 à 20 % des établissements bancaires français seulement en sont équipés.

On peut d'ailleurs dresser une ligne de séparation entre pays latins et pays anglo-saxons : alors que la France, l'Italie et l'Espagne sont assez peu disciplinées dans ce domaine, et appliquent la directive a minima, la Grande-Bretagne, l'Allemagne, la Hollande et les pays scandinaves appliquent scrupuleusement ces obligations.

Améliorer le contrôle d'identité dans les banques

Donc les obligations réglementaires existent (heureusement) mais sur le terrain on se rend rapidement compte que seul le minimum est mis en œuvre. Manque de moyens ? Manque de sensibilisation ? Manque de formation ? Manque de volonté ? Manque de temps ? La sécurité coûte chère, même pour les banques. Elles préfèrent donc transférer le risque de fraude sur une assurance. Perdre du temps à vérifier un papier d'identité ou de comparer des signatures de chèques ne semble donc pas faire partie de leurs priorités.

Quoi faire alors ?

De nombreux témoignages sur Internet ou dans les médias traditionnels ont largement démontré que l'usurpation d'identité est un véritable fléau aujourd'hui.
Je ne rentrerai pas dans le débat lié aux nouvelles générations de papiers d'identité qui sont censées apporter une sécurité supplémentaire. Tout ce que je sais c'est que la biométrie n'aurait servi à rien dans le cas de la fraude dont j'ai été victime. Pourquoi ? Parce qu'un simple contrôle comparatif (la tête de l'escroc avec la photo de ma carte d'identité dont la banque a une copie) aurait suffi à démasquer le fraudeur. Pas besoin de haute technologie, juste d'une procédure simple, rapide et efficace. Je rajouterai même de bon sens.
Dans le cas des vols plus classiques de cartes ou de chéquiers, il faudrait peut-être penser à changer son fusil d'épaule et réfléchir à d'autres modes d'envoi de ces moyens de paiement. Privilégier les courriers recommandés ? Privilégier les envois directement à l'agence et l'envoi du code confidentiel par courrier recommandé (ou directement en agence) avec juste un e-mail ou un SMS indiquant au client qu'il doit se rendre à l'agence pour récupérer ces moyens de paiement ?
Dans tous les cas, la priorité est de renforcer les contrôles d'identité en agence bancaire. De la création de compte au retrait de carte bancaire en passant par les retraits d'espèces au guichet (ou les remises de chèques), ma petite expérience confirme une nouvelle fois (si je me fie aux témoignages publiés sur Internet par des centaines de victimes) que les moyens mis en place actuellement sont loin d'être suffisants.
Concernant plus globalement les fraudes aux cartes bancaires, j'insiste aussi sur le fait qu'il faut aller porter plainte. Même si ce n'est pas indispensable pour être dédommagé par la banque, il est important de montrer aux autorités l'importance des fraudes de ce type. Il me semble normal d'avoir, dans un Etat de droit, la possibilité pour une victime de porter plainte pour espérer un minimum de justice et ne pas donner aux fraudeurs en tout genre un sentiment d'impunité (qui reste assez vrai dans le cadre des délits commis sur Internet).
Etre victime d'usurpation d'identité peut transformer une vie en vrai cauchemar. Car ensuite, comment prouver son identité à la Justice ? Aux personnes qui vont vous réclamer de l'argent ? Usurper une identité en ligne est très simple. Usurper une identité dans la vie réelle n'est pas plus difficile. Internet a facilité l'achat de faux documents. La criminalité physique a rapidement trouvé en Internet un lieu de convergence avec la cybercriminalité. On trouve tout sur les forums cybercriminels : de la photocopie photoshopée (qui trompera déjà pas mal de services en ligne…) au vrai faux papier en passant par les justificatifs de domicile (facture de téléphone, d'électricité…).
Pour mon cas personnel, normalement je serai intégralement remboursé. Par contre, maintenant je sais que quelqu'un possède un faux document d'identité et qu'il peut usurper mon identité pour monter des arnaques et escroqueries en tout genre.

Vente pyramidale et escroquerie

La vente pyramidale est un système alléchant qui peut piéger des personnes ayant besoin de revenus complémentaires. Voici les quelques règles à connaitre pour éviter les arnaques, tant pour les consommateurs que pour les demandeurs d'emploi.

Définition de la vente pyramidale

Le principe de la vente pyramidale est celui de la création d'un réseau d'affaires qui a la particularité d'être vertical. Il s'agit pour une personne souhaitant vendre des produits de trouver des acheteurs potentiels qui deviendront ses filleuls, et qui auront à leur tour la possibilité de vendre les produits à leurs propres filleuls, et ainsi de suite. Ce système de parrainage implique la constitution d'un réseau auquel va s'agglomérer un nombre de plus en plus important de filleuls. Pour rejoindre le réseau, chacun d'entre eux devra le plus souvent payer une somme d'argent. Bien évidemment, le fonctionnement d'un tel système implique de faire croire en contrepartie aux filleuls (qui sont des parrains en devenir) qu'ils connaîtront la fortune rapidement.

Afin de faire grossir le réseau d'affaires, il n'est pas rare que certaines entreprises fassent diffuser des annonces d'emplois faisant miroiter des rémunérations astronomiques. Bien évidemment, ces annonces se gardent bien de préciser que les chiffres qu'elles énoncent ne peuvent jamais être atteints.

D'autres annonces, plus réalistes, laissent envisager un gain dont on ne connaît pas le montant précis, mais dont on sait qu'il sera très limité. Enfin, certaines annonces font état de la nécessité pour le futur parrain d'acheter des stocks de produits, du matériel de démonstration ou des guides de fonctionnement qui n'ont pour seule utilité que d'enrichir les personnes situées tout en haut de la pyramide d'affaires.

En pratique, les systèmes de ventes pyramidales sont très souvent proposés sur internet. Le plus souvent, ces annonces sont précédées d'un (faux) témoignage d'une personne censée s'être rapidement enrichie via un système de réseau. Pourtant, la plupart de ces annonces en ligne font la promotion d'une pratique considérée comme illégale en France ainsi que dans de très nombreux pays du monde.

Législation en France

La loi française est claire sur ce point. Les techniques de vente en réseau, pour être valides, doivent respecter les dispositions prévues par l'article L. 121-15 du code de la consommation. Or cet article interdit :

1° La vente pratiquée par le procédé dit « de la boule de neige » ou tout procédé analogue consistant en particulier à offrir des marchandises au public en lui faisant espérer l'obtention de ces marchandises à titre gratuit ou contre remise d'une somme inférieure à leur valeur réelle, et en subordonnant les ventes au placement de bons ou de tickets à des tiers ou à la collecte d'adhésions ou inscriptions ;

2° Le fait de proposer à une personne de collecter des adhésions ou de s'inscrire sur une liste en exigeant d'elle le versement d'une contrepartie quelconque et en lui faisant espérer des gains financiers résultant d'une progression du nombre de personnes recrutées ou inscrites plutôt que de la vente, de la fourniture ou de la consommation de biens ou services.

Pratiques interdites

En plus d'interdire le procédé de la boule de neige, l'article L. 121-15 du code de la consommation pose les interdictions suivantes :

- celle d'obtenir d'un adhérent ou affilié du réseau le versement d'une somme correspondant à un droit d'entrée ou à l'acquisition de matériels ou de services à vocation pédagogique, de formation, de démonstration ou de vente ou tout autre matériel ou service analogue, lorsque ce versement conduit à un paiement ou à l'attribution d'un avantage bénéficiant à un ou plusieurs adhérents ou affiliés du réseau.
- celle d'obtenir d'un adhérent ou affilié l'acquisition d'un stock de marchandises destinées à la revente, sans garantie de reprise du stock aux conditions de l'achat, déduction faite éventuellement d'une somme n'excédant pas 10% du

prix correspondant. Cette garantie de reprise peut toutefois être limitée à une période d'un an après l'achat.

Conclusion : les offres trop alléchantes sont souvent des arnaques.

Sanctions

L'article L. 132-19 du Code de la consommation sanctionne les ventes "à la boule de neige" d'une peine de 2 ans de prison et 300 000 euros d'amende. En outre, la personne condamnée s'expose à devoir rembourser à ceux de ses clients qui n'auront pu être satisfaits les sommes versées par eux.

Conseils

Certains signes doivent éveiller votre attention : une entreprise créée récemment, des produits de faible valeur réelle (ou de mauvaise qualité) ou des sommes importantes exigées à l'inscription sont autant d'indices qui doivent vous faire directement penser à une arnaque.

Qu'est-ce qu'une vente à la boule de neige ?

La vente à la boule de neige, également appelée vente pyramidale, est un système de vente par parrainage.

Il s'agit, dans un premier temps, de proposer un produit à un acheteur en lui faisant espérer qu'il obtienne cette marchandise à titre gratuit ou qu'il en obtienne le remboursement partiel (par remise d'une somme d'argent inférieure à la valeur réelle) à condition qu'il trouve un certain nombre de nouveaux acheteurs.

Dans un second temps, ces derniers devront, quant à eux, trouver à leur tour des acheteurs afin de bénéficier des mêmes avantages et ainsi de suite.

Ce système repose donc sur une progression constante du nombre d'acheteurs recrutés par les acheteurs eux-mêmes provoquant ainsi un effet boule de neige.

La vente à la boule de neige est interdite en France car elle est considérée comme une pratique commerciale illicite. Cette infraction est punie d'une amende de 4 500 euros et d'un emprisonnement d'un an. Une peine complémentaire de remboursement des sommes versées aux clients non satisfaits peut également être appliquée (C. consom. L. 122-6 et L. 122-7).

Arnaque à la progression géométrique

La vente pyramidale est une forme d'escroquerie dans laquelle le profit ne provient pas vraiment d'une activité de vente comme annoncé, mais surtout du recrutement de nouveaux membres. Le terme « *pyramidale* » identifie le fait que seuls les initiateurs du système (au sommet) profitent en spoliant les membres de base.

Ce système se camoufle fréquemment derrière les termes de « Vente multiniveau » ou « commercialisation à paliers multiples » (en anglais *multi-level marketing* ou « MLM »), bien que des différences fondamentales existent, qui permettent à certains pays d'interdire la vente pyramidale alors que la vente multiniveau reste permise (notamment en France grâce au statut de Vendeur à domicile indépendant (VDI).

Législation en France

La vente pyramidale (procédé dit de la « boule-de-neige » ou de la « chaîne d'argent ») est interdite en France depuis 1953 (Article L 122-6 du Code de la Consommation 1° et 2° alinéas). Ce texte a été complété par une loi du 1er février

1995 (3° et 4° alinéas) qui précise les interdictions concernant les réseaux de vente. Depuis cette date, une entreprise qui ne respecterait pas cette réglementation et aurait des pratiques illégales serait condamnée.
Selon la législation française, « Il est interdit de proposer à une personne de collecter des adhésions ou de s'inscrire sur une liste en lui faisant espérer des gains financiers résultant d'une progression géométrique du nombre de personnes recrutées ou inscrites » (art. L. 122-6 et art. L. 122-7 du code de la consommation) et « cette interdiction est assortie de peines d'amende ou de prison. »

Financement du terrorisme : le crowdfunding en ligne de mire

Le dernier rapport du Sénat sur les réseaux djihadistes pointe le manque de contrôle des plateformes de financement participatif. Ce qui fait bondir les acteurs du secteur.
A la lecture du rapport du Sénat sur la lutte contre les réseaux djihadistes, Nicolas Lesur a bondi. Un paragraphe en particulier a retenu l'attention du président du Financement participatif France (FPF), association des professionnels du crowdfunding français. Il pointe "les risques de financement d'activités terroristes liées à l'activité du financement participatif" :
Cette technique de financement pourrait, dans les années à venir, favoriser des dérives [...] du fait d'un manque de régulation des opérateurs".
La commission d'enquête recommande donc de revoir le cadre juridique de cette pratique de financement et d'accroître la surveillance des opérateurs.
"De l'irresponsabilité !"
Pour Nicolas Lesur, ces soupçons sont totalement infondés : Des sénateurs désignent le crowdfunding comme outil de radicalisation ! C'est de l'irresponsabilité ou de l'incompétence !"
Il rappelle pour convaincre qu'"aucun acte terroriste n'a été financé par une plateforme de crowdfunding française". Et rappelle « Le financement du terrorisme dans le monde, c'est plusieurs milliards de dollars par an, le crowdfunding en France, c'est 150 millions d'euros. On est loin de créer une machine à laver qui va financer allègrement le djihadisme international !"
Pourtant, le rapporteur et sénateur PS, Jean-Pierre Sueur, persiste et signe auprès de "L'Obs" : Nous avons des suspicions très fortes, sans doute des indices de financement de terrorisme par de nombreuses sortes de financement participatif. Il est très facile de détourner le crowdfunding de son objet."
Alors qu'en est-il vraiment ? Le crowdfunding finance-t-il le djihad, en France ou ailleurs ?
Des campagnes sur Twitter
Vrai qu'aucune affaire de ce genre n'a été signalée en France. Mais vrai aussi que le boom du crowdfunding n'a pas échappé aux réseaux djihadistes. Face à l'arsenal déployé par les services de renseignement du monde entier pour lutter contre son financement, le terrorisme s'est rabattu sur des outils plus discrets, plus difficiles à surveiller par les autorités.
Dans un rapport publié en février 2015, le Gafi (Groupe d'action financière) montre que le financement du terrorisme (mais aussi des conflits armés en tout genre) via les réseaux de communication modernes et l'utilisation de techniques de crowdfunding, a considérablement augmenté au cours de la dernière décennie.

Le Gafi prend pour exemple le département médias de l'Etat islamique (EI), Al Hayat Media center, qui a lancé plusieurs campagnes sur Twitter dans le but de recueillir des fonds sur une plateforme dédiée. A la manière des grandes entreprises de crowdfunding, cette plateforme a créé des statuts "or" ou "argent" pour valoriser et récompenser les contributeurs les plus généreux.

Finance-t-on un projet ou une cause ?

Le mélange des genres n'est jamais loin. En 2012, le site spécialisé américain Wired a révélé que la plateforme américaine Kickstarter avait relayé l'appel aux dons de Matthew VanDyke, ancien journaliste américain qui a combattu aux côtés des rebelles libyens, pour financer un film documentaire sur ces opposants au régime de Bachar al-Assad. Le texte de présentation du projet indiquait simplement : "Deux combattants de la liberté de la révolution libyenne rejoignent le soulèvement syrien contre Assad et vont en faire un film."

Wired s'interrogeait : Est-ce qu'il s'agit de réunir des fonds pour aider la révolution ou pour aider à la réalisation d'un film sur la révolution."

Réponse de Matthew VanDyke : Le but de ce projet est de filmer pour soutenir les rebelles. Nous ne prévoyons pas de participer aux combats."

"Ils pourraient ne pas planifier de combattre. Mais ils pourraient avoir besoin de se battre si ça devait advenir", pointait le journal qui s'interrogeait encore sur les questions juridiques et politiques que soulevaient un financement de ce type, sur un terrain où des groupes djihadistes comme l'EI ou Jabhat al-Nosra combattent aux côtés des rebelles.

Le projet a été suspendu par Kickstarter après la publication de l'article de Wired.

L'ambiguïté sur la nature des causes financées a été soulignée en octobre 2014 par le directeur adjoint du service canadien du renseignement de sécurité (SCRS). Lors d'une audition devant le Sénat canadien, il a expliqué le fonctionnement de la collecte de fonds via le crowdfunding de candidats canadiens au djihad, sous le regard visiblement ahuri du sénateur qui l'interrogeait.

Lorsqu'il s'agit de particuliers, ces sommes sont relativement modestes, soit jusqu'à 10.000 dollars [...] Lorsqu'il s'agit d'organisations, vous êtes dans les six chiffres".

Comment la manoeuvre a-t-elle pu passer inaperçu ?

L'objectif de la récolte de fonds n'est pas nécessairement expliqué. [...] Ils le font parfois sous le couvert d'aide humanitaire par le biais du financement participatif. Alors, ils créent un site web et recueillent des fonds. […] Tant que les fonds ne sont pas utilisés, il est très difficile d'envisager des poursuites uniquement parce qu'il y a eu une collecte de fonds. C'est très bien caché."

Une réglementation renforcée en France

En France, à la différence des Etats-Unis où les plateformes comme Kikstarter, Indiegogo et Gofundme laissent tout partir en ligne, la régulation du crowdfunding impose de fortes contraintes pour les entreprises. La réglementation est identique à celles des établissements bancaires classiques, et les plateformes doivent savoir qui sont les porteurs de projet. L'ordonnance du 30 mai 2014 est venue renforcer la moralisation du secteur.

C'est la raison pour laquelle Arnaud Burgot, directeur général de la plateforme participative Ulule, juge très sévèrement l'alerte lancée par les sénateurs :

Oui, il y a un risque, mais comme dans toute activité financière. Nous sommes soumis, comme tous les établissements financiers, aux obligations de lutte contre le blanchiment et le financement de terrorisme qui s'appliquent sur les transactions bancaires."

Les obligations sont les suivantes :

- Les plateformes de crowdfunding n'ont pas le droit de collecter des fonds direct sans avoir un agrément. La plupart des plateformes choisissent de travailler avec un prestataire agréé, banque ou émetteur de monnaie électronique.
- Pour les virements, elles sont dans l'obligation d'identifier le bénéficiaire :

On ne verse pas d'argent à des personnes que l'on ne connaît pas !"

Par ailleurs, les plateformes ont de nombreux outils et indicateurs à la disposition pour détecter une transaction anormale : croisement des adresses IP d'où sont effectuées les transactions, des pays d'où sont censées avoir été émises les cartes bleues, analyse des volumes et de la vélocité des sommes déposées. Si un cas semble suspect, un examen complet est effectué. En parallèle, ces contrôles se font aussi au niveau des établissements bancaires affiliés.

Des opérateurs encore trop novices

Chez Tracfin, on admet bien volontiers que le crowdfunding n'est pas une zone de non-droit, contrairement à l'utilisation des bitcoins par exemple. Mais aussi que le risque est réel, tant la croissance du marché du crowdfunding est exponentielle.

Pour le service de renseignements, des failles existent. Ainsi, les opérateurs des plateformes de financement participatif ne sont pas aussi bien entraînés à une connaissance fine de leur clientèle que les opérateurs financiers classiques. A ce jour, ils n'ont ni les moyens, ni la vigilance, ni la culture en la matière des banques traditionnelles.

Quant au filet de sécurité que constitue la présence de banques adossées aux plateformes, il est considéré chez Tracfin comme insuffisant du fait de sa passivité :

Dans la majeure partie des cas, les établissements bancaires ne sont pas en contact direct avec les clients, ils connaissent moins bien l'origine et le destinataire des fonds, ils vont donc perdre de l'information."

Eric Vernier, professeur de finance et chercheur à l'Iris, a longtemps travaillé sur les techniques de blanchiment d'argent, souligne, pour sa part, une réglementation encore trop limitée :

A ce stade, il y a une absence évidente de contrôle et de suivi. Une fois la caisse remplie, les virements peuvent arriver n'importe où et aucune règle n'oblige à la réalisation du projet. Il sera d'autant plus difficile de contrôler un flux d'argent, s'il existe un tas d'intermédiaires entre le donateur et le bénéficiaire."

Tracfin sur le qui-vive

Dans ces conditions, et même si rien ne permet de mesurer l'ampleur du phénomène, le risque est pris très au sérieux. Eric Vernier :

Sur le plan macro-économique, les sommes qui pourraient transiter peuvent paraître dérisoire, mais on sait très bien qu'on n'a pas besoin de milliards pour organiser un attentat."

C'est précisément ce financement individuel de candidats au djihad qui constitue la principale source d'inquiétudes pour Tracfin. Les collectes de fonds de nature communautaire ou religieuses, qui visent un public spécifique, sont surveillées de près. Tout comme les appels aux dons pour des causes humanitaires.

La tâche est ardue, admet-on chez Tracfin : La différenciation entre soigner des enfants en Syrie et apporter de l'aide aux combattants djihadistes n'est pas évidente à faire. On ne veut pas remettre en cause la première finalité mais la seconde est problématique. Il y de grande difficultés de contrôlabilité."

Le contrôle est d'autant plus complexe que le service de renseignement de Bercy tâtonne encore sur les schémas possibles des transactions... C'est un "sujet en cours", assure-t-on au sein de Tracfin : Notre métier est de savoir quel temps il fera demain, et pour le moment il est difficile de savoir où, quand, et dans quel volume, la pluie va

tomber. Disons qu'on n'est pas sous la pluie, mais on commence à voir les nuages et il y a quelques gouttes."

Démarche éthique

De leur côté, les plateformes participatives les plus connues se sont engagées à poursuivre leurs efforts pour limiter les risques. Nicolas Lesur affirme : Nous avons tout intérêt à être vigilants, puisqu'il en va aussi de notre réputation."

L'association professionnelle qu'il préside a créé il y a deux ans "une charte déontologique régulièrement enrichie de bonnes pratiques", qui énonce des règles supplémentaires, "indépendamment de celles auxquelles nous sommes soumis". Un souci éthique qui a poussé les pouvoirs publics à créer un label "plateforme de financement participatif régulée par les autorités françaises". Une white list, en quelque sorte, à défaut de pouvoir dresser une black list