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 DES ACTUALITES INTERNATIONALES

DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Le Parlement européen va se pencher sur la blockchain

Le Parlement européen a validé la création d'un groupe de travail chargé de surveiller la blockchain et les crypto-monnaies, et de proposer des mesures de régulation. Ce groupe serait piloté par la Commission européenne.

Le Parlement européen a accepté la création d'un groupe de travail dédié aux crypto-monnaies et à la blockchain. L'objectif : surveiller ces technologies et recommander des mesures législatives. Conscient que la blockchain et les monnaies de type bitcoin représentent une opportunité tant pour le consommateur que pour l'économie, Jakob von Weizsäcker, eurodéputé du groupe de l'Alliance progressiste des socialistes et démocrates, met en garde contre le zèle législatif. "Pour ne pas étouffer l'innovation, nous préférons favoriser la surveillance de précaution plutôt que des réglementations préventives. C'est dans ce but que nous avons demandé à la Commission de créer un groupe de travail chargé de surveiller l'évolution de ces technologies, et de proposer en temps voulu des mesures de régulation", rapporte un article du site The Blockchain.

Lutter contre le blanchiment d'argent

Dans le cadre de la directive contre le blanchiment d'argent, la Commission européenne examine actuellement des propositions visant à imposer plus de transparence aux plateformes d'échanges de devises virtuelles, c'est-à-dire à lever l'anonymat associé à ce genre d'échanges.

Les institutions craignent que l'usage des crypto-monnaies et de la blockchain soit détourné à des fins criminelles (blanchiment d'argent et financement du terrorisme).

Publié le 31 mai 201

Liens : http://www.usine-digitale.fr/article/le-parlement-europeen-va-se-pencher-sur-la-blockchain.N394257

Lutte contre le terrorisme : Les 3 nouveautés à ne pas manquer !

Au cœur des préoccupations, la lutte contre le terrorisme connait un nouveau tournant avec cette loi du 3 juin 2016 visant à mettre en œuvre de nouvelles dispositions pour renforcer la prévention et la répression.

Plan détaillé :

1. Introduction
2. La mise en place de nouveaux moyens d'investigation
3. Le renforcement des contrôles
4. La lutte contre le financement du terrorisme

Une place particulière est accordée à la procédure pénale, élément fondamental dans un Etat de droit. En effet, garantissant l'effectivité du droit pénal, la procédure tend à protéger la société contre les actes qui lui portent atteinte. Son rôle est alors de garantir la cohésion et les valeurs, notamment, de la société, ainsi que de protéger les droits et les libertés des citoyens.

Outil aux mains de la justice afin de lutter contre tout type de criminalité**,** la procédure pénale doit s'adapter aux évolutions de la société et donc aux évolutions de la criminalité. Si elle a fait, ces dernières années, l'objet de nombreuses réformes, les divers attentats ayant touché douloureusement la France ont renforcé cette volonté d'adaptation de la procédure pénale afin de lutter efficacement contre le crime organisé**,** le *terrorisme* et ainsi institue des dispositions pérennes, applicables en dehors du cadre de l'état d'urgence.

Afin de répondre à cet objectif, un projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale a été présenté le 3 février 2016 par M. Jean-Jacques Urvoas, garde des Sceaux, ministre de la justice, et par M. Michel Sapin, ministre des finances et des comptes publics. Adoptée le 25 mars 2016, promulguée le 3 juin 2016 et publiée au Journal officiel du 4 juin 2016, cette loi *(1)* vient compléter celle du 24 juillet 2015 relative au renseignement *(2)*.

Ainsi, cette loi poursuit un triple objectif :

- le renforcement de la lutte contre la criminalité organisée et notamment le terrorisme par des mesures spécifiques de droit pénal et de procédure pénale pour améliorer la répression judiciaire et par des mesures préventives relevant de l'action administrative pour mieux détecter et surveiller la menace terroriste ;
- le renforcement des garanties au cours de la procédure pénale**,** spécialement au cours de l'enquête et de l'instruction (rôle du Procureur de la République), afin de la rendre conforme aux exigences constitutionnelles et européennes ;
- la mise en place de simplifications afin de faciliter le travail des enquêteurs et des magistrats.

La mise en place de nouveaux moyens d'investigation

Avec cette loi, les procureurs et les juges d'instruction pourront mettre en oeuvre de nouveaux dispositifs d'investigation. Ainsi, par exemple, il sera possible d'utiliser des dispositifs techniques de proximité pour capter des données de connexion. Le recours aux sonorisations, à la fixation d'images et la captation de données informatiques seront également envisageables dans le cadre des enquêtes diligentées par le parquet.

Les perquisitions de nuit dans les domiciles seront également possibles en cas de terrorisme et de risque d'atteinte à la vie, sous le contrôle d'un juge. De ce fait, les moyens auparavant réservés aux services de surveillance sont étendus à l'enquête et l'instruction.

En outre, cette loi vient améliorer la protection des témoins menacés. En effet, elle met en place, pour certains types de crimes (crime contre l'humanité, criminalité organisée) la possibilité pour l'autorité de jugement d'ordonner le huis clos le temps de l'audition d'un témoin. De plus, leur identification ne se fera pas au moyen de leur identité (nom, prénom) mais au moyen d'un numéro. En conséquence, si l'identité du témoin est connue des parties, elle ne sera pas rendue publique.

Enfin, cette loi renforce les conditions d'acquisition et de détention des armes. Dans ce cadre, outre l'interdiction d'acquisition pour certaines personnes, les "coups d'achat" seront autorisés. Il s'agit pour les enquêteurs d'acheter des armes pour révéler l'existence d'un trafic. Ainsi, le trafic d'armes, tout comme la cybercriminalité, est plus sévèrement combattu et réprimé.

Le renforcement des contrôles

Pour garantir la sûreté de l'Etat, diverses dispositions quant aux contrôles de certaines personnes ou de certaines installations sont mises en place. Ainsi, lorsqu'un grand événement est prévu, par exemple l'Euro 2016, des mesures peuvent être décidées afin de renforcer les contrôles d'accès aux installations. Ainsi, par exemple, sera-t-il possible de mettre en œuvre un système d'autorisation d'accès ou encore d'enquête administrative.

Encore, dans certaines conditions, la loi prévoit la possibilité pour un officier de police judiciaire d'inspecter et de fouiller les bagages des personnes faisant l'objet d'un contrôle d'identité *(4)*. De plus, lorsqu'il existe des doutes quant au comportement de la personne, qui laisse penser qu'elle peut être liée à des activités terroristes, elle peut faire l'objet d'une retenue sur place *(5)*.

Aussi, l'usage de caméras piétons est-il prévu pour les forces de police nationale et de gendarmerie, afin notamment de prévenir les incidents au cours des interventions. La caméra, portée de manière visible, enregistrera donc à titre préventif et pourra aussi permettre la constatation d'infractions. Elle pourra également être utilisée dans le cadre des poursuites. De ce fait, le but est ici à la fois de protéger les forces de l'ordre dans le cadre de l'exercice de leurs fonctions et de protéger le justiciable contre tout risque d'incidents ou de débordements *(6)*.

Enfin, les contrôles administratifs sont renforcés, notamment lorsqu'une personne s'est rendue ou a manifesté la volonté de se rendre à des endroits où ont lieux des activités, des opérations terroristes. Ce contrôle toutefois sera limité dans le temps (1 mois pour l'assignation à résidence, 6 mois pour la déclaration de domiciliation par exemple). La consultation habituelle de site faisant l'apologie du terrorisme ou provoquant la commission de tels actes sera également réprimée.

La lutte contre le financement du terrorisme

Mesure déterminante dans le cadre de la lutte contre le terrorisme, cette loi tend à lutter contre le financement du terrorisme en limitant la circulation d'importantes sommes d'argent. Pour ce faire, différentes mesures seront mises en place telles que la limitation des montants stockés sur les cartes prépayées ainsi que le renforcement du contrôle des opérations effectuées avec ces cartes.

En outre, les pouvoirs de Tracfin en la matière sont étendus. En effet, il sera, notamment, habilité à désigner, aux autorités compétentes, les personnes, physiques ou morales, ou les opérations présentant un risque élevé de blanchiment de capitaux ou de financement du terrorisme. De ce fait, les banques pourront mettre en place des mesures de vigilance à leur égard. Encore, Tracfin pourra obtenir des informations auprès d'entités gérant les systèmes de paiement. Le 06/06/2016,

Liens : http://www.net-iris.fr/veille-juridique/actualite/35232/lutte-contre-le-terrorisme-les-3-nouveautes-a-ne-pas-manquer.php

La tentation de maquiller les factures n'épargne aucun secteur. Les risques sont gros, du délit à la prison.

Fausses factures : « La confiance n'exclut pas le contrôle ».

Ce n'est un secret pour personne : la fausse facturation est une pratique courante de la vie des affaires. Ce maquillage comptable qui vise à authentifier une sortie de fonds partiellement ou totalement injustifiée emprunte différents schémas : majoration artificielle du prix d'un produit ou de travaux d'étude, paiement d'une commission à un intermédiaire sans prestation correspondante, constitution d'une caisse noire en franchise d'impôt dans un paradis fiscal, frais de traduction « bidon », etc. Les auteurs de tels montages destinés notamment à détourner des fonds privés ou publics ou à frauder le fisc encourent outre un redressement fiscal, des sanctions pénales pour faux et usage de faux, fraude fiscale, escroquerie, blanchiment, abus de bien social (ABS).

De l'abus de bien social à la fraude fiscale

L'exemple type d'ABS consiste pour une société d'un groupe à surfacturer ses prestations à une autre société ayant les mêmes dirigeants en vue de renflouer ses besoins en trésorerie. La fausse facture est aussi un outil d'abus de confiance relativement fréquent. C'est le cas par exemple d'un responsable des achats qui favorise l'un de ses fournisseurs en échange du « service » consistant, via la surfacturation de ses produits, à lui rétrocéder une partie des sommes perçues. Ou encore, du salarié qui paye une fausse facture à une société dont il sait qu'elle reversera une partie de cet argent à un fonctionnaire, en contrepartie de l'obtention d'un marché.

«*Les marchés publics sont un domaine dans lequel il existe des risques de corruption, il peut arriver, par exemple, qu'un sous-traitant ou un intermédiaire surfacture une partie de ses prestations, pour reverser une somme à un parti politique ou à un fonctionnaire* », souligne Sophie Scemla, avocate associée du cabinet Heenan Blaikie. Et leurs auteurs risquent gros : une loi du 6 décembre 2013 a porté les sanctions du délit de corruption à dix ans d'emprisonnement et 1.000.000 € d'amende, dont le montant peut être porté au double du produit tiré de l'infraction.

Reste que la tentation de maquiller ses chiffres de facturation n'épargne aucun secteur, dès lors que l'objectif est d'alimenter une « caisse noire » qui servira à verser des commissions, rémunérations et avantages à des tiers. Ou encore, de réaliser des économies d'impôt. C'est le cas des multinationales qui surfacturent des prestations de leurs filiales situées à l'étranger en vue de réaliser des transferts indirects de bénéfices en augmentant leurs charges en France. D'autres utilisent ce système pour augmenter la TVA déductible.

Contrôles internes et externes

A l'heure de l'informatisation de la comptabilité, les anomalies de facturation ne sont pas facilement repérables par les dirigeants.

Pour sécuriser les risques de fraudes et d'erreurs, les entreprises mettent en place des procédures dites de « contrôle interne ». Elles déterminent en amont la personne habilité à passer commande, celle qui signera le bon de commande, celle qui fera le rapprochement entre le bon de commande et le bon de livraison, puis celle qui, lors de l'enregistrement en comptabilité, retracera les différentes opérations et les rapprochera entre elles avant de délivrer le bon à payer. Ensuite, la personne dédiée au paiement remontera à son tour la chaîne des opérations. Cependant, toutes les entreprises n'ont pas la structure suffisante pour confier ces fonctions à des personnes différentes. « *On attire néanmoins l'attention de nos clients sur le fait que ce n'est pas au comptable qu'il faut confier les paiements. Il ne faut jamais perdre de vue que la confiance n'exclut pas le contrôle* », prévient Françoise Savés, expert-comptable à Bordeaux.

Par ailleurs, des contrôles externes sont effectués par des auditeurs légaux (commissaire aux comptes) ou contractuels (auditeur intervenant lors de l'entrée d'un

investisseur dans le capital, par exemple). « *La première chose que l'on vérifie est l'existence ou non d'une procédure de contrôle interne, cela nous permet de définir le périmètre de notre intervention* », explique Françoise Savés. Parmi les méthodes d'audit couramment utilisées : la « circularisation ». Concrètement, l'entreprise est invitée à écrire à 20 ou 30% de ses fournisseurs, préalablement sélectionnés par l'auditeur, et à leur demander de confirmer les mouvements enregistrés dans la comptabilité directement auprès du commissaire au compte. « *Cela permet de mettre en évidence d'éventuelles factures fictives avec des entreprises inexistantes, mais pas de révéler une collusion frauduleuse entre le fournisseur et l'entreprise* », précise Françoise Savés. En somme, aucune méthode n'est infaillible, leur vocation étant d'être le plus dissuasives possible ». Ainsi, lorsque l'expert met fin à sa mission, il exige du chef d'entreprise une « lettre d'affirmation » dans laquelle ce dernier assure avoir signalé tous les faits nécessitant un contrôle.

L'arrivée d'un nouveau salarié ou d'un nouveau dirigeant dans l'entreprise peut, de manière plus « accidentelle », mettre au jour des anomalies de facturation. Prenons le cas dans lequel l'une des filiales de la société embauche un nouveau directeur des achats. Ce dernier constate que cette filiale ne travaille qu'avec un seul sous-traitant depuis plusieurs années, de surcroit un sous-traitant plus cher que ses concurrents. En creusant, il se rend compte que la femme de l'ancien directeur des achats est actionnaire de ce sous-traitant qui en réalité surfacturait ses prestations. « *On est dans une situation typique d'abus de confiance et de corruption privée* » explique Me Scemla.

« L'effet boomerang »

Que doit faire le dirigeant informé d'une telle situation frauduleuse ? La dénoncer ? L'ignorer ? « *Toutes les factures qui n'ont pas été payées peuvent - et doivent - être contestées. Concernant celles qui ont été payées illégalement, le dirigeant n'est pas tenu de dénoncer l'infraction. En France, les personnes privées n'ont pas d'obligation de dénoncer au procureur des faits délictueux* », indique Me Scemla. D'autant que le pénal n'est pas forcément la voie judiciaire la plus opportune. « Le dirigeant qui s'aperçoit que la fraude provient de l'un de ses salariés peut bien sûr porter plainte contre lui. Toutefois, la société pourrait être mise en cause du chef de corruption si cette surfacturation avait servi à payer un pot de vin pour que la société obtienne un marché car c'est l'entreprise qui a bénéficié de la fraude : c'est ce qu'on appelle « l'effet boomerang », prévient l'avocate. Qui conseille, en fonction des circonstances, de recourir à la voie civile pour obtenir la restitution des fonds sur le fondement de la responsabilité contractuelle.

Liens : http://business.lesechos.fr/directions-generales/gouvernance/conseil-d-administration-surveillance/0203553882845-les-vrais-dangers-des-fausses-factures-100701.php

Société écran de facturation

Les sociétés écrans de facturation interviennent dans le cadre d'opération de commerce internationale. Ces sociétés interviennent lors de la vente ou de l'achat de produit pour le compte de la société mère. Elles agissent parfois sous le couvert d'une activité d'intermédiaire de commerce plus ou moins effective et effectuent des manipulations de prix qui permettent de transférer les prix dans les paradis fiscaux.

Il existe 2 méthodes de manipulation de prix :

- Majoration de prix d'achat à l'importation

- Minoration de prix de vente à l'exportation

Majoration abusive d'achat : une société française peut chercher à majorer le prix de son acquisition afin de réduire ses résultats imposable en France. Une société française A, importe du matériel en provenance d'un pays tiers B. La marchandise est livrée directement du pays tiers en France. La facturation est établie par une société E (membre du même groupe financier que la société A et son fournisseur), domiciliée dans un paradis fiscal, qui majore sensiblement le prix de vente facturé initialement par le fournisseur.

Cette pratique révèle un transfert irrégulier des bénéfices. Des montages plus complexes peuvent mettre en relation plusieurs sociétés écran afin de rendre plus opaques les transactions.

Minoration des ventes à l'exportation : des produits fabriqués par une société française A sont facturés à la société E établie dans un paradis fiscal au prix de 50, montant inférieur au prix de pleine concurrence qui s'élève à 100. Ces produits sont à nouveau facturés par la société E au clients B pour un montant de 100. Les produits sont directements expédiés par la société française A au destinataire final B.

Ce montage permet à la société A française de transférer dans un paradis fiscal sous couvert de la société E, un bénéfice de 50 qui aurait du normalement être imposé en France.

Liens : http://lutte-antiblanchiment.e-monsite.com/pages/techniques-de-blanchiment/societe-ecran-de-facturation.html

Sécurité bancaire : Les principales fraudes et arnaques des moyens de paiement

Carte bancaire, prélèvement, chèques, paiements en ligne, etc., tous ces supports de paiement vous exposent à la convoitise de nombreux escrocs.

Ces derniers développent tous les moyens (vol, arnaque, falsification, etc.) pour vous subtiliser un maximum de vos disponibilités financières.

Parfois il ne s'agit pas de vous voler vos supports de paiement mais de se procurer vos coordonnées bancaires voire simplement votre nom, prénom et adresse.

Une menace au quotidien

Les fraudes relatives aux moyens de paiement sont en constante progression. En 2012, les fraudes concernant les attaques de distributeur automatique de billets ont progressé de 73% et les fraudes sur les points de vente ont augmentés de 250%.

En France, 61% des opérations frauduleuses sont sur internet alors que les transactions sur internet ne représentent que 9,2% des transactions.

Il existe une multitude de moyens de subtiliser vos outils de paiement voire votre bien. Il est donc important de les connaitre pour éviter de se les faire subtiliser.

Vol de votre carte bancaire

Le saint Graal de tout fraudeur qui use des techniques les plus farfelues et les plus poussées pour se procurer toutes les informations relatives à votre carte bancaire

Piéger le distributeur automatique de paiement :

Le fraudeur installe un faux clavier sur le clavier du distributeur automatique de billet ou installe une fausse caméra de surveillance. Il récupère ainsi votre code secret que vous aurez tapé. Il lui suffit plus qu'à vous subtiliser votre carte bancaire. Souvent par la manière forte.

Certains vont encore plus loin en captant les informations directement sur votre carte bancaire en piégeant à la fois le clavier mais également le support de réception de votre carte bancaire du distributeur automatique de paiement ainsi il scanne votre carte bancaire à distance sans avoir besoin de vous voler votre carte bancaire.

L'œil qui louche

Lors de vos paiements chez des commerçants, dans une entreprise de restauration rapide par exemple, vous devez effectuer votre code secret en public. C'est à ce moment précis que l'œil « attentif » d'un fraudeur tente d'observer discrètement votre code. Il lui suffira par la suite de subtiliser votre carte.

Détournement du terminal de paiement chez le commerçant.

Certains fraudeurs poussent l'art du vol directement sur le lieu de vente. Cela fut le cas dans le sud de la France et plus particulièrement à Béziers où des terminaux de paiement chez des commerçants ont été discrètement échangés par des terminaux piégés.

Les fraudeurs récupéraient à distance toutes les informations relatives à votre carte bancaire y compris le code secret.

C'est près d'une dizaine de millions d'euros qui ont été détournés ainsi.

Complicité du commerçant

Certains fraudeurs arrivent à convaincre des commerçants de participer à leurs arnaques. Après avoir subtilisées les coordonnées d'une carte bancaire, les fraudeurs se rendent chez le commerçant-collaborateur pour effectuer des paiements nécessitant qu'une simple signature.

Détournement du courrier postal

Souvent les banques, particulièrement les banques en ligne, envoient votre carte bancaire par courrier postal. Il n'en suffit pas plus pour un fraudeur pour récupérer sans trop d'effort votre carte bancaire. Pour se faire, il intègrera les services postaux pour récupérer votre courrier ou bien il disposera d'un moyen pour accéder à votre courrier dans votre boite aux lettres.

Les distributeurs de courriers, de magazines et autres annuaires disposent d'une clé ouvrant le panneau des boites aux lettres. Une personne mal intentionnée peut ainsi accéder à votre courrier et parfois il aura la surprise d'y trouver vos clés de domicile qui lui permettront de rechercher tranquillement chez vous tous vos moyens de paiement sans que vous vous en rendiez compte.

Vol de chèque

Les chèques bancaires sont également un moyen de paiement que cherche à se procurer le fraudeur. En effet, votre chéquier présente votre nom, prénom et vos coordonnées. Il suffit alors de fabriquer une fausse carte d'identité reprenant ces informations pour ensuite l'utiliser à volonté.

Vol de votre chéquier

Le principal canal d'action pour récupérer votre chéquier reste bien entendu le vol. Le fraudeur tentera de récupérer celui-ci dans votre bagage (sac à main, sacoche d'ordinateur), dans votre vêtement (veste, manteau) ou dans votre véhicule de transport.

Mais certains fraudeurs n'ont pas froid aux yeux et peuvent aller jusqu'à la source pour récupérer votre chéquier. En témoigne l'exemple de ce fraudeur qui subtilisa à un client de la BNP Paribas du 13ème arrondissement de Paris, son courrier de convocation pour la récupération de son chéquier. Le voleur s'est présenté à l'agence avec une carte d'identité présentant toutes les coordonnées du client mais avec une photo différente. Il a fallu toute la vigilance de la conseillère d'agence qui connaissait

particulièrement bien son client pour éviter que ce dernier devienne la victime d'une fraude bancaire.

Faux chèque bancaire

Certains fraudeurs sortent tout droit du film « Attrape moi si tu peux » et sont capables de recréer des chéquiers à l'image d'une banque.

L'arnaque au faux chèque repose sur trois acteurs, l'expéditeur du chèque, le destinataire du chèque et la banque.

Dans le cadre d'une transaction, l'expéditeur (ou acheteur) fait parvenir un chèque avec une somme supérieure au montant de la transaction négociée. Il prétexte une erreur et demande à ce que le destinataire (le vendeur) lui retourne la différence moins les frais liés au dérangement dès que celui-ci aura déposé le dit chèque.

Une fois déposé, la banque du vendeur crédite la somme sur son compte. Rassuré le vendeur accepte alors de renvoyer l'excédent à son acheteur.

Ce dernier demande alors de passer exclusivement par des organismes tels que Western Union afin de récupérer au plus vite la différence.

Et ce n'est que quelques jours plus tard que votre banque vous informe que le chèque est faux.

Faux chèque de banque

Lors d'une transaction vous demandez un chèque de banque qui est pour vous une garantie. Une fois la transaction réalisée, vous déposez votre chèque de banque dans votre banque et découvrez que celui-ci est faux.

Vol des informations bancaires

Le vol de vos données est la principale activité des fraudeurs. Les fraudeurs s'ingénient à développer toutes les techniques possibles pour les récupérer.

En voici quelques unes :

Piratage informatique de votre ordinateur

Le classique du classique : Vous téléchargez un fichier qui contient un virus ou un cheval de Troie qui infecte votre ordinateur de manière soit à prendre le contrôle de celui-ci pour y récupérer des informations bancaires ; soit à vous observer en espérant que vous effectuerez un paiement en ligne afin d'enregistrer le plus simplement du monde les informations de la carte bancaire que vous taperez sur votre clavier.

Piratage d'un commerçant : Le commerçant se fait pirater son serveur. Et vos coordonnées bancaires se retrouvent entre les mains du pirate.

Email frauduleux

Vous recevez un email vous invitant à mettre à jour vos informations chez un de vos fournisseurs (EDF, Opérateurs téléphoniques, Banque, etc.) voire même des services des impôts.

Vous vous retrouvez sur une page quasi similaire à celle de votre fournisseur ou service des impôts dans lequel vous êtes invité à remplir vos coordonnées et vos informations bancaires.

Toutes ces informations sont récupérées en règle générale à l'étranger par un pirate informatique qui les utilise immédiatement pour réaliser des achats voire des virements bancaires.

Récupération via Wifi, NFC

Le développement des technologies permettant l'accès à distance favorisent la tentation des fraudeurs d'accéder à vos données.

Vos appareils de communication sont vulnérables à des attaques de pirates extrêmement bien équipés pour tenter de récupérer vos données lorsque vos appareils sont branchés en mode Wifi ou NFC.

Le développement du paiement mobile NFC qui permet de réaliser un paiement avec sa carte de paiement ou son téléphone portable équipée sans avoir à taper son code est une véritable aubaine pour les fraudeurs. Ces derniers n'ont plus besoin de vous subtiliser votre code secret ou de vous voler votre carte bancaire. Il leur suffit de développer les bons outils pour tenter de récupérer les informations de votre carte bancaire ou de votre mobile, puis de les dupliquer sur un support.

Arnaque sur Paypal

Paypal est un moyen de paiement prisé par toutes celles et tous ceux qui ne souhaitent pas communiquer leurs informations bancaires sur des sites de vente.

Le compte paypal étant limité par un montant défini, il est impossible pour un fraudeur ayant accès à ce compte de se servir sans limite.

Toutefois, les arnaques utilisant le service de paiement paypal sont nombreuses. Principalement sur les sites de vente de particulier à particulier.

Sur ces sites, l'escroc se porte rapidement acquéreur d'un objet en vente. Il propose l'envoi de la somme via paypal. Le vendeur reçoit une confirmation du transfert par email. Cet email peut être à la fois un vrai courrier provenant de paypal ou un faux courrier provenant de l'escroc.

Rassuré, le vendeur envoie alors l'objet à une adresse souvent un point relais ou à l'étranger.

Après l'envoi, le vendeur se rend compte que son compte paypal n'est pas réellement crédité. Ou bien il reçoit un vrai courrier de Paypal quelques jours plus tard lui indiquant que le transfert est bloqué car basé sur 'un moyen de paiement douteux.

Entretemps, le fraudeur disposera de votre bien qu'il pourra revendre ou utiliser à loisir.

Comme nous avons pu le voir les techniques de détournement de vos disponibilités financières sont très nombreuses.

Prendre connaissance de ces techniques d'escroquerie via les moyens de paiement est indispensable pour pouvoir les éviter.

Nos prochains articles vous donneront des conseils pour vous aider à vous en prémunir et des explications sur la manière de réagir lorsque l'on en est victime.

Liens : http://www.challenges.fr/services/choisir-ma-banque/20140326.CHA1982/securite-bancaire-les-principales-fraudes-et-arnaques-des-moyens-de-paiement.html

Assemblées de la BAD : Un plan de lutte contre les financements illicites

Les assemblées annuelles de la Banque africaine de développement se sont clôturées vendredi 27 mai à Lusaka, en Zambie. Ce commet qui a réuni chefs d'Etats et ministres africains, a été marqué par le lancement d'un Plan de lutte contre les financements illicites. Il vise à mettre un terme à l'évasion fiscale, à la corruption, mais aussi aux trafics illicites qui dans certains pays sont devenus un véritable pan de l'économie. C'est notamment le cas dans le Sahel où les trafics de bétail, de cigarettes, de carburants ou de drogues financent notamment les groupes terroristes.

Les revenus des trafics illicites dans le Sahel se comptent en milliards de dollars. Mais pour les Etats ils représentent des pertes colossales. « *Nous avons dû au Niger multiplier par plus de dix notre budget alloué à la sécurité en cinq ans, ce qui a un impact sur les ressources que nous pouvons allouer à d'autres secteurs tels que*

l'éducation, la santé ou le développement des infrastructures, etc. », explique Aïchatou Boulama Kané, ministre du Plan du Niger.
Ainsi le budget du Niger finance surtout des patrouilles des forces armées aux frontières du pays. Car le Niger est au cœur d'un corridor de trafic en partie contrôlé par des groupes terroristes. « *Il y a des trafics de cigarettes, etc. Aussi nous saisissons régulièrement dans le corridor venant de la Libye en direction du Mali ou dans le sens inverse. Il y a un véritable commerce illicite de drogues ou même d'armes. Nous arrivons à sécuriser nos frontières, ça ne veut pas dire qu'on est arrivés à un trafic zéro, mais quand même nous avons réduit ces trafics-là* », affirme-t-elle.
D'après les Nations unies, le trafic de cocaïne seul dans Sahel a généré 900 millions de dollars de revenus entre 2013 et 2014.

Lutter contre la corruption

La corruption et l'évasion fiscale minent également les économies africaines. D'après une étude de la BAD, entre 2000 et 2009, près de 30,5 milliards de dollars ont ainsi fuité hors du continent. Pour chaque dollar d'aide au développement perçu, les pays africains en perdent dix.
Depuis 2011 la lutte contre ces flux financiers illicites est inscrite dans la Constitution du Niger. « *Pour nous au Niger, financement illicite ça veut dire tout ce qui concerne la fraude fiscale, la corruption, l'argent qui disparaît et tous les détournements de manière générale,* précise Aichatou Boulama Kané. *Nous avons fini l'élaboration de notre plan d'action et nous comptons le soumettre bientôt au gouvernement pour l'adoption. Mais depuis 2011 nous avons mis en place tout un dispositif. Nous avons une Haute autorité de lutte contre la corruption et l'impunité qui a été créé. Nous avons tout un dispositif au plan juridique et au plan institutionnel. Maintenant il faut mettre tout cela en musique pour être efficace dans la lutte. Le Niger en 2011 était 134e dans l'indice de perception de la corruption. Nous avons gagné 28 places et nous sommes à la 106e place.* ». Publié le 27-05-2016.
Liens : http://www.rfi.fr/afrique/20160527-assemblees-bad-plan-lutte-contre-financements-illicites-trafics

Mauritanie : Séminaire sur l'identification du financement du terrorisme et le blanchiment d'argent

Les travaux d'un séminaire sur l'identification du financement du terrorisme et le blanchiment d'argent à l'échelle international à travers le système bancaire ont débuté mercredi à Nouakchott.
Le séminaire, de trois jours, est organisé par la commission d'analyse des informations financières (CANIF), relevant de la Banque Centrale de Mauritanie (BCM), en collaboration avec l'ambassade des Etats-Unis (USA) à Nouakchott et vise à permettre aux cadres de la CANIF, aux inspecteurs de la BCM et aux agents des banques agréés auprès de la dite commission de renforcer leurs capacités en matière de lutte contre le blanchiment d'argent et le financement du terrorisme au niveau du milieu bancaire mauritanien.
Les participants sont encadrés, au cours de ce séminaire, par des experts de la Mauritanie et des USA spécialisés dans la lutte contre le blanchiment d'argent et le financement du terrorisme.
Le gouverneur adjoint de la BCM, M. Cheikh El Kebir Ould Moulaye Taher a, à cette occasion, souligné que ce séminaire s'inscrit dans le cadre des efforts consentis par

notre pays pour identifier les risques des fonds générés à travers le crime organisé, le trafic des drogues et le terrorisme.
Il a, par la suite, ajouté que ces efforts visent, en premier lieu, à protéger l'économie nationale, à immuniser notre système financier contre les tentatives de son exploitation dans le blanchiment d'argent généré à travers ces crimes et d'autres sources illicites.
Le gouverneur adjoint de la BCM a indiqué que la Mauritanie qui accorde une grande importance à ce sujet à l'instar de la communauté internationale a ratifié plusieurs conventions en la matière.
Il a ensuite indiqué que la BCM, suivant les instructions du Président de la République, Monsieur Mohamed Ould Abdel Aziz, veille à la mise en place des systèmes adéquats garantissant la protection et la stabilité de la société et de l'économie nationale.
Pour sa part l'ambassadeur des USA auprès de notre pays, SEM. Larry André a indiqué que la Mauritanie constituera un danger pour les intérêts des terroristes lorsqu'ils sachent que ce pays dispose de fonctionnaires bien-formés et déterminés à priver les terroristes des sources de financement originelles et des sommes recueillies de leurs crimes.
L'ambassadeur a ajouté que les mauritaniens seront plus à l'aise lorsque leur pays deviendra plus sécurisé face à ces défis qui dérangent le monde entier, notant que le trafic de drogue et les autres opérations illicites constituent une source de financement pour les actes terroristes.
La cérémonie d'ouverture du séminaire s'est déroulée en présence du secrétaire général de la CANIF, M. Mohamed Ely El Keihel et d'autres responsables du système bancaires en Mauritanie. 2 juin 2016.
Liens : http://www.maghrebemergent.info/actualite/breves/fil-maghreb/59761-mauritanie-seminaire-sur-l-identification-du-financement-du-terrorisme-et-le-blanchiment-d-argent.html

Les caisses d'épargne volent au secours de la marijuana

Flairant la bonne affaire, des caisses d'épargne aux Etats-Unis volent au secours de l'industrie lucrative du cannabis en proposant des services bancaires chèrement facturés malgré les avertissements des autorités.
C'est dans le nord-ouest, région progressiste où les deux usages de la marijuana - médicale et récréative- sont autorisés, que ces établissements s'activent le plus pour organiser un secteur estimé à plus d'une vingtaine de milliards de dollars à l'horizon 2020.
La grande majorité des transactions commerciales (salaires, commandes, impôts) sont toutefois acquittées en liquide car la détention, l'achat et la vente de cannabis restent illégaux au niveau fédéral, incitant le secteur bancaire traditionnel à s'en détourner.
Mais depuis 2014, les cultivateurs et les propriétaires de dispensaires de cannabis peuvent néanmoins ouvrir un compte bancaire professionnel auprès de certaines caisses d'épargne habilitées. Ils peuvent ainsi transférer et recevoir de l'argent, payer par chèque et en endosser, effectuer des dépôts et des virements.
"Il est dans l'intérêt de tous qu'ils puissent gérer en toute sécurité leurs affaires", explique à l'AFP Kelli Hawkins de Numerica Credit Union, l'une des pionnières de

cette mini-révolution saluée par le milieu du cannabis où l'on égrène le nom des commerces refoulés comme des "pestiférés" par les grandes banques.

"Blacklisté"

Donald Morse, président du lobby Oregon Cannabis Business Council et propriétaire du dispensaire Human Collective à Portland, s'est vu fermer des comptes au moins cinq fois par Bank of America et Wells Fargo.

"Quand vous voulez ouvrir un compte auprès d'une banque, elle vous demande la nature de votre commerce. Si vous êtes honnête et répondez +cannabis+, c'est non! On se retrouve à garder soi-même son argent. Chaque mois, je m'expose à une agression (car) je dois trimbaler du cash au bureau des impôts pour payer la taxe de 25% sur les ventes du cannabis à usage récréatif", raconte M. Morse.

Las, il a fini par mentir sur ses activités mais le pot aux roses a été découvert. "Je suis blacklisté maintenant", s'emporte-t-il.

L'extrême prudence des grandes banques, échaudées par leurs milliards de dollars d'amendes pour pratiques illicites liées à la crise de 2008, va jusqu'à pousser des promoteurs immobiliers à refuser de louer des locaux à l'industrie du cannabis par peur d'être sommés de rembourser précipitamment leur emprunt.

Sollicitées par l'AFP, les banques indiquent qu'elles ne veulent pas courir le risque de perdre leur licence, parce qu'une directive de février 2014 du FinCEN (département du Trésor) n'exclut pas des poursuites judiciaires.

"Forcer des chefs d'entreprises qui opèrent légalement au vu de la législation de l'Oregon à transporter des sacs de sport remplis d'argent est une invitation au crime et au délit. Ceci doit cesser", dénonce le sénateur démocrate Jeff Merkley, auteur avec trois autres parlementaires d'une proposition de loi généralisant les services bancaires à l'industrie du cannabis.

Odeur

En attendant, les établissements intéressés doivent investir des milliers de dollars dans la gestion de ces comptes à risques, car ils doivent fouiller dans le passé de ces clients particuliers, passer au crible les relations dispensaires/fournisseurs, contrôler les sorties et entrées de fonds, vérifier les chiffres de ventes communiqués aux autorités locales et les dépôts bancaires.

Et si, en principe, l'argent n'a pas d'odeur, certaines caisses d'épargne comme Maps Credit Union dans l'Oregon exigent que les coupures déposées ne sentent pas le cannabis.

Chez Salal à Seattle, "nous demandons un premium et des frais mensuels (supplémentaires) pour couvrir les coûts de gestion", explique Carmella Houston, une responsable. Ces "comptes sont taxés fortement pour qu'ils puissent être rentables", justifie-t-elle.

Malgré ces conditions, les demandes affluent: depuis 2014, Salal a reçu plus de 2.000 requêtes mais n'a ouvert que 200 comptes.

La start-up Kind Financial, associée à Link to Banking qui s'emploie à développer les services bancaires liés au cannabis, veut exploiter le filon.

Elle propose aux banques un logiciel leur fournissant "des informations en temps réel sur leurs clients et aussi sur les clients de leurs clients pour se conformer à la législation anti-blanchiment", avance son patron David Dinenberg.

Est-ce suffisant pour les autorités? "Notre tâche est de déterminer si les caisses d'épargne évaluent et gèrent correctement les risques", répond John Fairbanks du NCUA, le superviseur des caisses d'épargne. 08 mai 2016. Avec AFP

Liens : http://www.voaafrique.com/a/aux-etats-unis-les-caisses-d-epargne-volent-au-secours-de-la-marijuana/3320434.html

La FinCEN aux États-Unis émet 2 nouvelles directives contraignantes

La FinCEN, l'autorité américaine contre les crimes financiers a émis cette semaine 2 nouvelles directives qui pourraient avoir un impact négatif sur les entreprises dans le marché du Bitcoin.

Dans l'un de ces directives, la FinCEN atteste que les sites d'échanges qui font affaire aux États-Unis de même que les entreprises étrangères qui ont des clients américains, doivent obligatoirement s'enregistrer comme des entreprises de transmission d'argent ***(Money Services Business).*** Cette règle s'appliquerait aussi pour les entreprises opérant des machines Bitcoin et même ceux qui opèrent des sites mettant en relation des acheteurs et des vendeurs sans qu'aucune somme d'argent en dollar ne soit transféré!

La première directive était attendue par la communauté: à l'heure actuelle, plusieurs entreprises en opération ont déjà mis en place les moyens pour être considérés comme des MSB. De plus, certaines compagnies étrangères ont arrêté d'offrir des services aux clients américains en prévision de cette réglementation…C'est la deuxième directive qui a pris tout le monde par surprise:

En effet, toute entreprise qui facilite le transfert et la conversion de bitcoin sera obligée de s'enregistrer comme une MSB! Cette règle qui ratisse large aura, entre autres, un impact sur les activités de Bitpay qui se croyait exempté de cette réglementation. Maintenant, la compagnie devra s'enregistrer comme une MSB dans chacun des états où elle opère, ce qui pourrait lui coûter relativement cher. Bitpay est un intermédiaire de paiement qui accepte les bitcoins des clients pour les transférer par la suite sur la plateforme du commerçant où le produit a été acheté.

Après avoir lu le document, il est difficile de savoir quels sont tous les facteurs qui obligent une entreprise dans l'écosystème du Bitcoin à s'enregistrer comme une MSB. La FinCEN recommande aux compagnies dans le doute de s'informer de leur statut auprès d'elle pour éviter de mauvaises surprises.

Reste à voir si la réglementation au Canada ira dans la même lignée que celle aux États-Unis…

Liens : http://aleny.net/la-fincen-aux-etats-unis-emet-2-nouvelles-directives-contraignantes/#post_content

L'argent de Daech entre banques et microtransferts

Selon plusieurs rapports rédigés ces derniers mois, les djihadistes ont mis la main sur les établissements financiers dans les zones qu'ils contrôlent en Irak et en Syrie. De quoi leur permettre d'accéder aux zones grises du système international.

Repoussée à une date ultérieure, la maintenance des systèmes informatiques du Trésor américain. Un courrier électronique signé d'un de ses départements, celui de la lutte contre les crimes financiers (le Financial Crimes Enforcement Network – Fincen), l'a annoncé vendredi soir, juste après les attentats de Paris. Objectif affiché : vérifier dans les bases de données utilisées par les institutions financières d'éventuelles transactions douteuses liées aux terroristes. Mardi, tout en refusant de répondre sur la nature

précise des résultats obtenus lors de ces investigations, Jennifer Shasky Calvery, la directrice du Fincen, a souligné que l'examen des bases de données permet de mieux comprendre les flux financiers entre l'«État islamique» (EI) et les « terroristes combattants étrangers » qui partent dans les territoires contrôlés par les djihadistes en Syrie et en Irak. Selon elle, les requêtes font remonter plus de 1 000 signalements chaque mois, contre 800 au printemps. « Je peux vous dire que les informations enregistrées par nos institutions financières sont extrêmement précieuses », insiste-t-elle.

La majeure partie des ressources de Daesh est tirée de la prédation des matières premières

Réunis à Antalya (Turquie), le week-end dernier, les dirigeants des États membres du G20 placent officiellement la lutte contre les circuits de financement du terrorisme au premier rang de leurs priorités. Mais comment faire face à Daech qui, moins lié qu'al-Qaida à de riches mécènes du Golfe, tire la majeure partie de ses ressources de la prédation des matières premières, comme le pétrole, le blé ou l'orge, ainsi que de « taxes » diverses et variées, de rançons, de ventes d'« esclaves », de pillages pratiqués à grande échelle dans les territoires qu'il occupe en Irak et en Syrie (lire aussi l'Humanité du 17 novembre) ? Alors que les États composant le G20 promettent une « coopération renforcée sur l'échange d'informations et le gel des avoirs » des terroristes, tout un pan des mouvements financiers que l'on peut relier à l'organisation djihadiste demeure encore très nébuleux, en fait. Et les rapports produits ces derniers mois par diverses institutions internationales, comme le Groupe d'action financière sur le blanchiment de capitaux (Gafi), ou nationales, comme celui du Congrès états-unien, ne lèvent qu'un coin du voile.

Sur les territoires contrôlés en Syrie et en Irak, Daech s'est emparé de centaines d'établissements bancaires. Derrière la confiscation de l'équivalent en dinars d'un demi-milliard de dollars en espèces, selon une évaluation réalisée par les services américains, c'est en fait l'accès au système bancaire et financier international, avec toutes ses zones grises et ses paradis fiscaux, qui a de quoi préoccuper. D'après le Gafi, après la prise de Mossoul, la deuxième ville d'Irak, en juin 2014, la plupart des banques implantées dans les régions prises par Daech ont transféré à Bagdad tous leurs centres d'opérations en lien avec le système financier international. De quoi accréditer l'idée avancée par certains observateurs que, sous le joug de l'«EI», les rares établissements bancaires encore en activité se limitent à des opérations de dépôt… Cela dit, le Sénat américain s'inquiète tout de même du fait que les opérations de virement ou de change de devises demeurent possibles. En Syrie, toujours selon le rapport du Gafi qui date de février 2015, comme plus d'une vingtaine d'établissements financiers continuent leurs activités, «il y a des juridictions avec lesquelles les banques opérant sur les territoires occupés par l'"EI" arrivent à maintenir des liens», mais, avertit l'institution, «une part très significative des informations récoltées sur ce terrain n'ont pu, de par leur nature très sensible, être inclues dans le rapport public ».

C'est le système basé sur l'opacité et le camouflage de l'argent qu'il faudrait changer

Entre la hawala, un système informel et traditionnel de compensation bancaire répandu dans tout le sous-continent, et des campagnes de financement plus ou moins déguisées sur les réseaux sociaux, Daech apprécie, d'après toutes les investigations des institutions internationales, la discrétion des systèmes de transfert d'argent et de devises : les opérations sont certes limitées quant à leurs montants, mais elles sont difficilement détectables. Selon le Gafi, «l'EI" peut détourner le système,

spécialement quand les banques sous son contrôle perdent leur accès au système financier international». D'après les constats des experts, l'argent transite d'Irak ou de Syrie ou vers l'Irak et la Syrie par le biais des agences implantées dans les régions périphériques de sa zone de contrôle, voire des États voisins. Lors du G20, Michel Sapin, le ministre français des Finances, a plaidé pour resserrer les mailles du filet en traquant les transferts de faibles montants pouvant servir à financer des attentats. Dans le secteur passablement dérégulé des transferts d'argent et de devises, la tâche promet d'être extrêmement ardue. Et tous les efforts de « coopération », d'« échange d'informations » ou d'« accès aux bases de données » des banques n'y suffiront pas. C'est le système basé sur l'opacité des circuits financiers et le camouflage de l'argent qu'il faudrait changer

Liens : http://www.humanite.fr/largent-de-daech-entre-banques-et-microtransferts-590336

Baron du cannabis, Costa del Sol et penthouse de luxe... Qui est Sofiane Hambli, l'indic sulfureux des stups ?

Ce trafiquant de drogue, considéré comme l'un des plus gros importateurs de haschich en Europe, était aussi l'informateur de l'ancien numéro 1 de la lutte antidrogue.

C'est un petit monde où chacun a son surnom : Mohamed Benabdelhak, dit "le bombé", Djamel Talhi, alias "Johnny Depp", Mohamed Bouarfa alias "l'autruche" et Sofiane Hambli, aka "la Chimère". Ce dernier, comme ses compères, appartient au cercle fermé des millionnaires du cannabis. Comme un certain nombre d'entre eux, il est actuellement derrière les barreaux.

Depuis son plus jeune âge, Sofiane Hambli alterne prison et vie de pacha, en France, en Espagne ou au Maroc. Cet homme de 40 ans, né en 1975 à Mulhouse (Haut-Rhin), est considéré comme l'un des plus gros importateurs de cannabis en Europe. Il est aussi, selon *Libération* et i-Télé, l'informateur de l'ancien numéro 1 de la lutte antidrogue, François Thierry.

Un penthouse de 250 m2 avec piscine sur le toit

Son nom ressurgit à l'occasion de l'une des plus grosses saisies en matière de cannabis, en octobre 2015, à Paris. Sept tonnes de résine sont alors découvertes dans trois camionnettes garées boulevard Exelmans, dans le très chic 16e arrondissement. Une facture et des traces ADN conduisent les douanes jusqu'à Sofiane Hambli, qui occupe un penthouse de 250 m2 avec piscine sur le toit, boulevard Exelmans. Un environnement digne du célèbre film *Scarface*, LA référence cinématographique des caïds.

Le locataire, qui selon *Libération* réglait en cash le loyer de 9 000 euros par mois, s'est volatilisé. *"C'est la plus grosse prise depuis longtemps"*, se félicite François Hollande. Problème, le trafiquant s'avère en réalité être un indic de l'Office central pour la répression du trafic illicite de stupéfiants (OCRTIS), enregistré au Bureau central des sources. Un *"cador"* du trafic international de drogue, *"capable de toutes les audaces"*, selon une source judiciaire, et bien connu des services de police.

Le "baron de l'or vert" ou le "Mulhousien", ses deux autres sobriquets, a grandi à Bourtzwiller, un quartier de la ville haut-rhinoise. Il fait partie, selon le journaliste Jérôme Pierrat, de cette poignée de caïds des cités, qui se sont hissés avec une rapidité fulgurante au sommet du marché de la drogue, *"au détriment des anciens du milieu traditionnel"*.

Shit, immobilier et voitures de luxe

A 22 ans, Sofiane Hambli est déjà l'un des principaux revendeurs de haschisch marocain dans la région alsacienne. Il va échapper de peu à un coup de filet en juin 1997, dans le cadre d'une vaste opération anti-drogue menée par les gendarmes, baptisée "Paco68". Sofiane Hambli part en cavale, direction l'Espagne et sa Costa del Sol, un repère pour les trafiquants en tous genres. Comme l'écrit *Le Monde,* dans un dossier consacré au grand banditisme, les petits voyous devenus grands *"ont élu ce bout de côte espagnole comme refuge. Porte d'entrée de l'Europe du Sud, c'est sur les plages alentour que se font, toutes les nuits ou presque, les livraisons de cannabis"*.

Sofiane Hambli se planque dans la ville andalouse de Marbella et sa jolie marina Puerto Banus, à quelques encablures du Maroc. Dans ce paradis pour célébrités et princes saoudiens, mais aussi pour groupes mafieux internationaux, le Français fait prospérer ses affaires. Selon *Les Dernières nouvelles d'Alsace,* il réinvestit dans l'immobilier et le négoce de véhicules haut de gamme l'argent provenant du trafic de shit. Belles filles, belles voitures, belles villas... Sofiane Hambli mène la grande vie.

La justice française, elle, ne l'oublie pas. En juillet 1999, il est jugé et condamné par défaut à huit ans de prison pour trafic de haschich. Il faudra trois ans aux autorités judiciaires pour remettre la main sur l'affranchi. En mai 2000, la saisie de 300 kg de drogue à Vienne (Isère) permet de retrouver sa piste. Il est finalement arrêté en Espagne puis extradé en France en février 2002. Sofiane Hambli fait immédiatement opposition au jugement qui l'a condamné à huit ans de prison. Sa peine est ramenée à cinq ans de prison trois mois plus tard.

Trafic en prison puis évasion

C'est dans ce contexte qu'il rencontre l'avocat Alex Civallero. Joint par francetv info, ce dernier se souvient d'un jeune *"très actif, souriant, avec un contact facile"*. Son client le tutoie d'emblée. Et se montre averti en matière de procédure.

Il sait ce qu'il peut tirer d'une personne. Il est manipulateur.

L'avocat Alex Civallero

à francetv info

Pas question, pour Sofiane Hambli, d'arrêter son business derrière les barreaux. En juin 2002, un téléphone portable est découvert dans sa cellule de la prison de Mulhouse, ce qui lui vaut d'être transféré à Saint-Mihiel, dans la Meuse. Le détenu est alors placé sur écoute. Les enquêteurs l'entendent négocier la vente de *"50 caisses"* à un intermédiaire, et promettre à un acolyte de lui *"trouer les genoux avec une perceuse"* après le vol supposé d'une tonne et demie de marchandise.

Selon les *DNA*, Sofiane Hambli charge son petit frère Hakim de récupérer des dettes auprès d'une dizaine de Marocains et d'Espagnols, pour un total de 6 millions d'euros. En octobre, il est mis en examen pour trafic de haschich, avec la complicité de sa famille... et de son avocat. Alex Civallero, renvoyé devant la justice pour lui avoir transmis des puces de téléphone contre rémunération, sera finalement relaxé.

En août 2003, Sofiane Hambli, qui purge désormais sa peine à Metz-Queuleu, prétexte des douleurs au poignet. Il est transféré à l'hôpital pour une radiographie. A la sortie de la consultation, un homme à moto surgit et menace les surveillants avec une arme factice. Sofiane Hambli saute à l'arrière du deux-roues et les deux hommes prennent la fuite.

Opération "baleine blanche"

Le Mulhousien s'envole de nouveau vers la Costa del Sol et reprend ses affaires. Il échappe à plusieurs tentatives d'arrestation. En 2004, les policiers espagnols mènent une opération contre son équipe au cours de laquelle trois tonnes de cannabis sont

saisies. Interpellé, Sofiane Hambli réussit tout de même à s'enfuir après une fusillade durant laquelle un policier est blessé par balle. En 2005, une cinquantaine de personnes sont arrêtées et plus de 200 propriétés et véhicules de luxe saisis lors de l'opération "baleine blanche", la plus grosse jamais organisée contre le crime organisé et le blanchiment d'argent sur la Costa del Sol. Là encore, Sofiane Hambli échappe au coup de filet. Mais comme l'indique *Le Parisien*, plusieurs documents saisis attestent qu'il trempe dans plusieurs affaires immobilières louches autour de Marbella.

En attendant, la justice suit son cours. En mars 2007, il est condamné par défaut à dix-huit ans de prison pour le trafic de drogue en prison. Deux ans plus tard, les policiers espagnols retrouvent sa trace. Sofiane Hambli réapparaît en Espagne après s'être caché quelques mois au Maroc. Localisé à Benahavis, un village situé sur les hauteurs de Marbella, il est interpellé lors d'un déplacement en bord de mer. L'arrestation est mouvementée. Le fugitif, en possession d'un faux passeport et de 210 000 euros en liquide, tente d'effacer ses empreintes digitales en se frottant les doigts sur les barreaux de sa cellule. Selon i-Télé, c'est pendant sa détention en Espagne que Sofiane Hambli a été recruté par François Thierry, alors directeur de l'OCRTIS.

Extradé vers la France, il est incarcéré au centre pénitentiaire de Nancy-Maxéville en janvier 2011. Jugé en sa présence, cette fois, il voit sa peine de dix-huit ans de prison ramenée à treize ans. Sofiane Hambli est alors défendu par Anne-Claire Viethel, spécialiste en droit immobilier. Selon *Libération*, elle est aussi accessoirement la compagne de François Thierry. *L'Est républicain* rapporte que le gros bonnet devient un détenu modèle et reçoit la visite de "costumes-cravates" en prison. Il profite de passe-droits, comme un portable dans sa cellule. A la fin 2014, après cinq ans et dix mois de détention, il bénéficie d'un régime de semi-liberté et rejoint la région parisienne.

"Logisticien" hors pair

Qu'a-t-il fait depuis sa libération complète en 2015 ? Nul doute que ce "logisticien" hors pair dans le transport de la drogue entre le Maroc et la France a remis le pied à l'étrier. L'a-t-il fait en partie pour le compte des stups de la police judiciaire ? La question fait grincer des dents au sein des hautes instances de la lutte anti-drogue, régulièrement secouées par des affaires illustrant les relations dangereuses entre "tontons" et "policiers". Un risque proportionnel à la place de l'informateur dans la hiérarchie de la voyoucratie.

On n'a jamais eu un indic avec une piscine sur le toit en plein Paris !

Un ancien cadre de la PJ de Lyon à France tv info

Une guerre des polices est à l'œuvre quant à la place des indics dans les enquêtes. Et la saisie des 7 tonnes de cannabis en plein Paris en est un épisode supplémentaire. Selon plusieurs sources, les douaniers ont volontairement court-circuité cette "livraison surveillée" de l'OCRTIS pour dénoncer les méthodes de leurs collègues, qui flirtent avec la légalité. Ces "coups d'achat" visent à laisser passer une certaine quantité de drogue sur le territoire, avec la complicité d'un trafiquant-indic, en vue d'interpeller le réseau de revendeurs. Mais dans le cas de l'affaire des sept tonnes, aucune interpellation n'a eu lieu, si ce n'est celle de Sofiane Hambli, arrêté le 22 février dernier à Gand (Belgique).

Extradé par hélicoptère comme Salah Abdeslam

Le baron de la drogue a été extradé, sous haute surveillance, par hélicoptère de la Belgique vers la France, quelques jours avant Salah Abdeslam. Les deux hommes ont d'ailleurs été représentés par le même médiatique avocat, Sven Mary. En France, c'est Joseph Cohen-Sabban qui assure la défense de Sofiane Hambli. Sollicité par France tv info, il a refusé de parler au nom de son client, indiquant avoir *"reçu un mandat très*

précis à cet égard". Devant les enquêteurs, Sofiane Hambli *"est resté très évasif, laissant simplement entendre qu'il avait toujours agi sous les ordres de l'OCRTIS",* indique *Libération.*
"Ce mec a 40 millions d'euros sur des comptes un peu partout en Europe. Ils lui ont créé un réseau logistique d'importation. Pourquoi ?", s'interroge un ancien responsable des stups auprès de France tv info. Et de s'inquiéter pour les suites judiciaires de l'affaire : *"Hambli parle de l'OCRTIS comme de ses 'employeurs'. Il risque dix-huit ans de prison, il n'hésitera pas à aller raconter des saloperies sur les policiers."* Alex Civallero estime, au contraire, que son ancien client *"saura se faire discret et se montrer conciliant, pour s'extirper de la situation"*. Sofiane Hambli n'est sans doute pas fini.
Liens : http://www.francetvinfo.fr/societe/drogue/baron-du-cannabis-costa-del-sol-et-penthouse-de-luxe-qui-est-sofiane-hambli-l-indic-sulfureux-des-stups_1469315.html

Paiements internationaux : Swift prépare sa mue 2.0

La messagerie bancaire sécurisée s'engage à effectuer les transferts d'argent internationaux en un jour d'ici un an. 21 banques expérimentent de nouveaux processus d'échanges entre elles.
Le système de messagerie bancaire sécurisée Swift prend le taureau par les cornes. La coopérative de banques et d'institutions financières, dont l'infrastructure est utilisée par près de 11.000 membres dans quelque 200 pays pour garantir l'échange de données financières réalisé lors d'un paiement ou d'un achat de titres, a décidé de « *réinventer les paiements internationaux sur la base de nouveaux standards* ». Elle a lancé pour ce faire en décembre dernier un plan baptisé « Global payment innovation initiative » auquel se sont ralliées 45 banques fin janvier.
Sur ces 45 établissements qui couvrent 67 % des échanges transfrontaliers traités par Swift, 21 lancent un pilote qui doit d'ici l'automne faire la preuve que le réseau de banques correspondantes de la messagerie, vieux de près de 45 ans , reste pertinent et compétitif face à de nouveaux entrants.
Les chiffres clefs
45 institutions financières se sont engagées à adopter de nouvelles règles d'échanges à partir de 2017.
67% des paiements internationaux traités par Swift devraient alors être réalisés en un jour.
En pratique, les établissements participants s'engagent à ce qu'un transfert d'argent par une grande entreprise cliente, fait au sein du réseau international des banques pilotes, soit crédité en un seul jour ouvré. C'est en effet là que le bât blesse : une opération qui transite via Swift prend aujourd'hui au minimum trois jours et le délai peut aller jusqu'à neuf jours selon la complexité du transfert. Ce, sans que le client ne soit informé sur l'état d'avancement de l'opération ni assuré du délai exact pour que l'argent transféré le soit réellement, ni qu'il soit sûr du coût précis de l'opération. Ces incertitudes sont devenues incompréhensibles voire intolérables dans un monde où l'instantanéité est devenue la norme. Elles font d'ailleurs le succès de nouveaux acteurs comme Transferwise ou Paypal.
Plan stratégique
« *La messagerie Swift n'est pas du tout en cause, ce sont les pratiques des banques du réseau en matière de transfert qui doivent être réinventées* », souligne Thierry

Chilosi, responsable Market initiatives chez Swift. Autrement dit le fonctionnement du réseau de banques correspondantes chargées d'acheminer le transfert doit être sérieusement dépoussiéré et c'est ce à quoi se sont engagés les 21 établissements du pilote via un corpus de nouveaux accords de services multilatéraux proposés par Swift. Cet ensemble de règles devra être validé à la conférence annuelle Sibos organisée par la messagerie internationale à Genève fin septembre, avant d'être étendu aux 45 banques volontaires en 2017.

En parallèle Swift va lancer en mai une réflexion afin de définir une stratégie à cinq ans sur la manière dont la messagerie peut intégrer de nouvelles technologies afin d'améliorer la qualité et le coût de son service. Cela étant, Swift ne craint pas d'être balayé par des innovations comme la Blockchain qui permet de valider des transactions sans passer par un tiers de confiance. « *La technologie ne suffit pas, elle permet d'adresser la question du transfert lui-même mais pas tout ce qui tourne autour et notamment les sujets liés à la lutte contre le blanchiment* », prévient Stanley Wachs, directeur international de l'innovation dans les paiements chez Swift.

Liens : http://www.lesechos.fr/finance-marches/banque-assurances/021765608971-paiements-internationaux-swift-prepare-sa-mue-20-1206874.php

Financement du terrorisme : Les banques invitées à renforcer leurs contrôles

Les banques sont notamment invitées à mieux surveiller les transferts d'argent effectués par des clients occasionnels à destination de la Syrie, de l'Irak ou d'autres territoires exposés au risque de blanchiment et de financement du terrorisme.

C'est une initiative qui tombe à point nommé. Tracfin, la cellule antiblanchiment de Bercy, et l'autorité de tutelle des banques devaient publier, vendredi 20 novembre, une liste précise et renforcée des obligations s'imposant aux banques et autres établissements financiers en matière de lutte contre le financement du terrorisme et l'argent sale. L'Etat islamique est visé au premier chef.

Fondé sur une vigilance accrue des clients et des déclarations de soupçons élargies, ce plan d'action vise à mieux enrôler les banques dans la détection des flux illicites. Un rôle que leur a assigné le législateur depuis la fin des années 1990 et dont l'importance ne cesse de se renforcer avec la mondialisation financière et la montée du terrorisme.

Elaboré à la demande de Michel Sapin, ministre des finances, après les attentats contre *Charlie Hebdo* et l'Hyper Cacher de Vincennes, ce document de 62 pages (dans sa version courte) prend tout son sens aujourd'hui, alors qu'il se trouve publié, par un hasard du calendrier, une semaine après les attentats du 13 novembre. Selon nos informations, ce plan avait été validé juste deux jours avant les attaques terroristes de vendredi.

« Les changements dans l'attitude d'un client, doivent alerter »

« Beaucoup de leçons peuvent être tirées des dramatiques attentats à Paris et en région parisienne, qui doivent nous conduire à une mobilisation totale. Face à ces actes barbares, je veux rappeler la détermination de la Banque de France à participer à la lutte contre le terrorisme, en s'attaquant à son financement », déclare François Villeroy de Galhau, nouveau gouverneur de la Banque de France et président de l'Autorité de contrôle prudentiel et de résolution (ACPR). *« Je n'ai pas de doute que l'implication du secteur financier dans* [la] *mise en œuvre* [de ce plan] *sera totale, nous y veillerons avec les professionnels »,* poursuit-il.

Concrètement, ce document va de la surveillance des transferts d'argent effectués par des clients occasionnels à destination de la Syrie, de l'Irak ou d'autres territoires exposés au risque de blanchiment et de financement du terrorisme aux opérations soudaines et inexpliquées de clients réguliers et sans histoire, en passant par la vérification poussée des documents d'identité ou attestations fournies.

« Les changements dans l'attitude d'un client, doivent alerter, mettent en garde les autorités. *Le financement du terrorisme peut s'appuyer sur une grande variété d'opérations : virements domestiques ou internationaux, transferts d'espèces, retraits, opérations de change, ouverture ou fermeture de comptes, opérations de crédit, dont l'une des principales caractéristiques est de porter sur de faibles montants financiers. »*

L'argent anonyme, une des clés du problème

Il s'agit en fait de rappeler le devoir fondamental des banques de *« connaître leurs clients »* et de vérifier la cohérence des transferts ou rapatriements de fonds opérés. Et ce, de bout en bout. Une obligation collective et globale dont les récents scandales financiers en matière de fraude et d'évasion fiscales (HSBC, LuxLeaks, etc.) ont montré qu'elle n'était pas toujours scrupuleusement assumée.

« L'ACPR et Tracfin appellent tout particulièrement l'attention des organismes financiers sur la lutte contre le financement du terrorisme, écrivent en préambule ces autorités de tutelle et de renseignement financier. (…) *Il est attendu qu'ils exercent une vigilance renforcée sur les transferts de fonds en provenance et surtout à destination de zones géographiques considérées comme risquées en matière de terrorisme ou de financement du terrorisme ou sur les opérations effectuées dans ces zones. »*

Les autorités rappellent aux banques et compagnies d'assurances que leurs dispositifs de contrôle doivent *« intégrer les risques liés* [à ces] *pays ». « Il leur incombe aussi »* de vérifier que certains Etats ne soient pas utilisés comme des *« pays de transit », « pour cacher le pays final de destination ou de provenance des fonds ».*

L'argent anonyme étant une des clés du problème dans le financement des actes terroristes – utilisation d'espèces et de cartes prépayées, pour payer personnes ou matériel… –, des déclarations systématiques sont prévues, notamment au-delà de 1 000 euros pour les opérations effectuées à partir de versements d'espèces ou au moyen de monnaie électronique.

Finalement, les superviseurs invitent banquiers et assureurs à *« suivre l'actualité nationale et internationale, les communiqués du ministère des finances et les rapports annuels de Tracfin ou du GAFI [*Groupe d'action financière, organisme intergouvernemental antiblanchiment] *»*

Liens : http://www.lemonde.fr/economie/article/2015/11/20/financement-du-terrorisme-les-banques-invitees-a-renforcer-leurs-controles_4814094_3234.html

Une surveillance des monnaies virtuelles afin de combattre le blanchiment et le terrorisme

La Commission européenne devrait mettre en place un groupe de travail pour superviser les monnaies virtuelles, comme le Bitcoin, afin de prévenir leur usage dans le cadre d'activités de blanchiment et de financement du terrorisme, a déclaré le Parlement dans une résolution non contraignante votée ce jeudi.

Le texte rédigé par Jakob von Weizsäcker (S&D, DE) suggère que la Commission développe une expertise relative à la technologie des monnaies virtuelles, et

recommande une législation. Il met cependant en garde contre une régulation excessive d'une technologie qui peut offrir des opportunités significatives pour les consommateurs et l'économie.
“Afin d'éviter d'étouffer l'innovation, nous préférons une surveillance de précaution plutôt que la régulation préventive. Cependant, les innovations dans le domaine des TIC peuvent se répandre très rapidement et devenir systémiques. C'est pourquoi nous appelons la Commission à établir un groupe de travail pour surveiller activement la façon dont la technologie évolue et proposer la régulation adéquate si le besoin s'en fait sentir”, a déclaré M. Von Weizsäcker.
La Commission examine des propositions pour intégrer les plateformes d'échange de monnaies virtuelles dans le cadre de la directive existante contre le blanchiment, qui sera prochainement mise à jour. Ces propositions prévoient l'obligation faite aux plateformes de mettre fin à l'anonymat lors d'un transfert d'une monnaie réelle à une monnaie virtuelle. Les régulateurs craignent en effet que le système existant ne facilite le blanchiment et les activités d'organisations terroristes.
La résolution du Parlement fut adoptée par 542 voix pour, 51 contre et 11 abstentions.
26-05-2016.
Liens : http://www.europarl.europa.eu/news/fr/news-room/20160524IPR28821/Surveillance-des-monnaies-virtuelles-pour-combattre-blanchiment-et-terrorisme

Paiements mobiles : Comment les rêves de blanchiment d'argent des criminels risquent de devenir réalité

À l'automne 2013, la justice américaine annonçait le dénouement de la plus grande affaire de blanchiment d'argent en ligne de l'histoire, avec l'inculpation des dirigeants du site de change Liberty Reserve, considéré comme « la plus grande banque pour criminels ». Plus d'un million de clients sont passés par cette société basée au Costa Rica pour blanchir plus de 6 milliards de dollars. Outre les trafiquants de drogue, Liberty Reserve était le repère de nombreux bandits et organisations criminelles spécialisées dans la fraude aux investissements et à la carte bancaire, l'usurpation d'identité, le piratage informatique et la pédophilie.
Si les plates-formes comme Liberty Reserve sont désormais placées sous haute surveillance, les paiements mobiles échappent encore au contrôle des autorités et services de police. Des millions de personnes, notamment dans les pays en développement, utilisent désormais leur téléphone mobile pour réaliser leurs opérations bancaires, et leur nombre augmente quotidiennement. Cette communauté mobile possède son lot de criminels qui, d'après certains spécialistes, se livrent à des activités tout aussi variées que dans le cas de Liberty Reserve, mais à moindre échelle — pour l'instant.
« Les paiements mobiles sont la nouvelle grande technique de blanchiment d'argent à laquelle nous allons avoir affaire », déclare John Cassara, qui a travaillé pendant 26 ans comme agent de la CIA et enquêteur sur les délits financiers au département du Trésor des États-Unis. « Les services de police du monde entier ont du mal à prendre les choses en main car le problème est encore mal maîtrisé et peu documenté. Mais tôt ou tard, nous y serons tous confrontés. »

Les services de police du monde entier ont du mal à prendre les choses en main car le problème est encore mal maîtrisé et peu documenté.

Voici le problème : La mise en place de réseaux bancaires et de télécommunications fixes coûte cher. C'est l'une des raisons pour lesquelles seulement une personne sur cinq parmi les 7 milliards d'habitants de la planète a directement accès aux banques et services financiers. Or, on dénombre 5 milliards de téléphones mobiles qui pourraient servir de porte-monnaie virtuels ou de distributeurs automatiques personnels. D'ici 2020, certains spécialistes estiment qu'il y aura 50 milliards d'appareils connectés et que les transactions mobiles seront privilégiées dans la plupart des pays d'Afrique, d'Asie et d'Amérique latine.

Pays où la corruption et la criminalité transnationale font rage et où les trafics en tout genre se multiplient. « Le phénomène va s'amplifier », ajoute John Cassara, qui a rédigé deux ouvrages sur le financement du terrorisme ainsi qu'un rapport du Département d'État américain sur les paiements mobiles (2008), et dispense désormais des conseils aux administrations et multinationales sur le sujet. « L'engouement pour les transactions mobiles va porter un sérieux coup aux cartes bancaires et aux distributeurs automatiques, tout en ayant un impact majeur sur les techniques de dissimulation et de blanchiment d'argent. » Le problème, ajoute-t-il, c'est que « personne ne se soucie vraiment de la manière dont les criminels vont pouvoir tirer parti de ces paiements mobiles. »

Comment tout cela fonctionne : Il suffit de prendre l'exemple du Kenya, où Safaricom a lancé en 2007 l'un des premiers programmes de paiement mobile, baptisé M-Pesa (« Pesa » signifiant « argent » en Swahili). M-Pesa compte à présent 15 millions d'utilisateurs, qui virent plus d'un milliard de dollars par mois vers l'Afrique de l'Est. Ce modèle est repris par plus de 50 autres pays, dont le Brésil, l'Afghanistan, l'Inde et une grande partie de l'Afrique.

Au Kenya, des milliers d'échoppes vendent des recharges de communication pour téléphones mobiles, qui se présentent généralement sous la forme de cartes à gratter. Plus de 60 000 d'entre elles sont d'ailleurs membres du programme M-Pesa, dépassant largement les 840 agences bancaires du pays. Les transactions annuelles réalisées via M-Pesa représentent plus de 20 % du PIB. Les clients échangent du liquide contre de la valeur qu'ils injectent dans leur téléphone, qui fait alors office de porte-monnaie électronique ou de carte virtuelle. Ils peuvent ainsi payer leurs factures, faire des achats, effectuer des virements, et surtout, faire créditer leur carte.

C'est à la fois simple d'utilisation et généralement moins onéreux que les services de transfert classiques. Les travailleurs étrangers peuvent toucher leur salaire par téléphone et verser l'argent à leur famille en quelques secondes. Les voyageurs peuvent déposer des espèces et les retirer dans un autre pays. Nombreuses sont maintenant les grandes banques qui s'empressent d'incorporer les paiements mobiles dans leurs services, au même titre que les multinationales comme McDonalds, Starbucks et la Western Union.

Les paiements mobiles sont très répandus dans les pays où les lois anti-fraude et anti-blanchiment et leur application laissent à désirer.

Les failles du système : Les paiements mobiles sont très répandus dans les pays où les lois anti-fraude et anti-blanchiment et leur application laissent à désirer. L'identification des clients n'est généralement pas très poussée, et le système de reporting financier du pays est souvent contourné. Même si elles possèdent l'expertise nécessaire — ce qui n'est pas le cas selon John Cassara et d'autres — les autorités n'ont donc quasiment aucun moyen de surveiller les paiements mobiles.

Par ailleurs, les transactions s'opérant via des téléphones mobiles et par SMS, rien ne permet de les tracer et encore moins de réunir des preuves pour engager des poursuites. Comme l'expliquait John Cassara lors d'un congrès en mai 2012, les criminels ont toujours gravité autour du maillon faible du système financier, jetant à présent leur dévolu sur les paiements mobiles. Au Kenya, le programme M-Pesa a été utilisé pour blanchir de l'argent, verser des pots-de-vin à des fonctionnaires corrompus et faciliter toutes sortes d'activités criminelles tels que les kidnappings et les extorsions de fonds. En guise de réponse, Safaricom a exigé de la part de ses clients, notamment ceux qui utilisent des cartes prépayées pour leur service de téléphonie, de lui communiquer davantage d'informations.

Mais s'il n'y a pas encore vraiment de quoi prouver que les paiements mobiles favorisent les actes criminels, « c'est tout simplement parce que personne ne surveille les transactions », avance John Cassara. En Afrique, en Asie, en Europe et aux États-Unis, les autorités financières semblent pourtant d'accord sur ce point et ont d'ailleurs exprimé leurs inquiétudes dans de récents rapports, témoignages officiels et interventions publiques (paywall). Elles s'inquiètent particulièrement de l'essor des paiements mobiles dans les pays où l'hawala, autrement dit le système de transfert de fonds informel, freine leurs efforts en matière de lutte contre le financement du terrorisme. Au Pakistan, par exemple, où 90 % des adultes n'ont pas de compte en banque, le prestataire de services financiers Easy Paisa compte plus de 100 millions d'abonnés. John Cassara parcourt le monde et finit l'une de ses présentations en disant : « Tout le monde est inquiet. Tout le monde acquiesce et a conscience du problème qui se profile à l'horizon, mais personne ne bouge. »

Liens : http://www.sas.com/fr_fr/insights/articles/risk-fraud/m-payments-machine-criminals-dreams.html

Blanchiment d'argent : Le paiement mobile est à surveiller (Centif)

L'expansion de technologies nouvelles ou en développement présente des risques potentiels de blanchiment de capitaux. Cela a été révélé, hier, par Me Fatou Soumaré, une consultante de la Centif au cours d'un séminaire de restitution d'études conduites en 2013 sur les risques de blanchiment de capitaux et de financement du terrorisme dans des domaines d'activité.

Travaillant sur la question du paiement mobile, la consultante a relevé quelques facteurs de risques de blanchiment dans les activités de paiement mobile. Il s'agit de l'impossibilité de mener, a priori, un contrôle du fait que les acteurs de supervision ne sont pas encore au fait des technologies employés, mais surtout de l'absence d'un contrôle adapté au dynamisme du secteur. Une situation qui, aux yeux de Me Soumaré, est une des réalités qui peuvent affecter l'efficacité de la supervision dès lors que la téléphonie mobile a acquis une place de choix dans le cœur des sénégalais.

L'identification des acheteurs et utilisateurs de services de téléphonie mobile recommandée

Citant le dernier rapport d'analyse du marché des télécommunications publié par l'Artp dans lequel il apparait qu'au 31 décembre 2012 le taux de pénétration du mobile est à 94,24% contre 76.62 en décembre 2011, Me Soumaré a indiqué que cela équivaut, à un parc de plus de 11 millions d'abonnés sur une populations totale de 13 millions de personnes pour trois exploitants de réseaux de téléphonie mobile. A ce propos, elle a préconisé une approche adaptée aux nouveaux produits et moyens

électroniques de paiement qui sont totalement dématérialisés et fonctionnent à distance et en temps réel.
Dans son étude, la consultante qui dit avoir observé quatre facteurs de risques qui sont l'anonymat, la rapidité, la mauvaise supervision et l'insaisissabilité, a préconisé une réflexion proactive. Une réflexion qui devra, selon elle, être menée et des actions entreprises dans l'objectif de réduire autant que possible, les risques de blanchiment de capitaux illicites et financement du terrorisme dans le secteur des services financiers mobile au Sénégal. Elle préconise ainsi la bonne application du décret N°2007-937 relatif à l'identification des acheteurs et utilisateurs de services de téléphonie mobile offerts au public.
Liens : http://www.seneweb.com/news/Telecommunication/blanchiment-d-rsquo-argent-le-paiement-mobile-est-a-surveiller-centif_n_135454.html

Mali. Paiement mobile : Un essor qui inquiète les Banques

Simples, rapides, faciles d'accès, les solutions mobiles de transfert d'argent connaissent un grand succès. Encouragés par l'engouement du public, certains opérateurs du secteur n'hésitent pas à empiétersur les plates bandes des établissements bancaires
A Bamako, tout comme dans le pays profond, la monétique, avec l'un de ses produits phares : le transfert d'argent et le paiement mobile, commence à bien s'ancrer dans les habitudes. En effet, aujourd'hui, en dehors des banques de la place, nombreux sont les opérateurs qui interviennent dans le secteur du transfert d'argent : des opérateurs de téléphonie mobile (Orange à travers OrangeMoney et Malitel travers Mobicash) qui le font sous le couvert de la BICIM et de la BIM, à ceux de l'informel en passant par les établissements agréés par la Banque centrale (Lemonway, Wari), leurs activités ont pris une telle ampleur qu'elles sont devenues un sujet de préoccupation pour les banques. Commentant la situation, un interlocuteur dira : « Ces opérateurs, à travers les kiosques qui poussent à Bamako comme des champignons, sont tellement confortés dans le transfert d'argent que certains d'entre eux commencent à s'investir dans la création de comptes similaires à des comptes bancaires, alors qu'ils n'ont pas vocation à le faire ».
Quels sont les facteurs qui ont favorisé la vulgarisation du transfert d'argent ? Quels sont ses avantages et ses inconvénients ? Quel impact sur les activités des banques ? Quelles solutions?
La monétique ou monnaie électronique est l'ensemble des solutions technologiques et informatiques permettant d'automatiser les transactions financières de façon très sécurisée. Sa vulgarisation a incontestablement des avantages et contribue sans doute à l'amélioration du quotidien des citoyens, explique le président de l'Association professionnelle des banques et établissements financiers (APBF), Moussa Alassane Diallo qui est aussi le PDG de la BNDA. La gratuité de la souscription pour l'ouverture de compte téléphonique, la proximité et la rapidité du service (les kiosques sont présentement visibles à chaque coin de rue) ainsi que la facilité pour les petits épargnants de pouvoir mettre de côté leur argent sont les principaux facteurs qui ont révolutionné le transfert d'argent et encouragent la bancarisation d'une partie de la population.
Selon le président de l'APBF, les banques ont pour objectif la vulgarisation de la bancarisation de l'économie malienne et depuis des années, elles envisagent de

réaliser 20% de taux de bancarisation de l'économie. En dépit des efforts, ce taux se situe aujourd'hui autour de 15%, souligne-t-il. D'où l'adoption d'une nouvelle stratégie appelée inclusion financière. Donc, on est passé de la notion de bancarisation à celle d'inclusion financière qui se traduit par le fait que les citoyens peuvent effectuer des opérations financières avec ou sans compte bancaire. Par exemple, à travers OrangeMoney, sans avoir de compte en banque, on peut envoyer de l'argent à un parent. Le receveur au village ne possède également pas de compte en banque mais reçoit son argent. Autre avantage de l'inclusion financière, le taux d'accès de la population à la finance est actuellement de l'ordre de 35%-36% contre 14-15% pour la bancarisation. Cette dernière implique l'ouverture d'un compte, alors que l'inclusion financière permet une plus grande vulgarisation des produits et services bancaires et l'accessibilité des populations aux opérations financières. Concernant l'impact des transferts sur les banques, le président de l'APBF souligne qu'ils sont de deux ordres : d'abord, ils diminuent la masse d'argent dans la circulation bancaire, ensuite ils occasionnent des pertes de commission pour le système bancaire. A titre d'exemple, lorsqu'un client demande à sa banque de transférer un ou deux millions de Fcfa, la structure gagne une commission sur l'opération.

De nombreux risques. S'agissant des nombreuses personnes faisant du transfert dans la rue, les quartiers ou au grand marché et qui ne sont enregistrées nulle part, les banquiers attirent l'attention sur le fait qu'elles opèrent dans l'illégalité. Par ailleurs, le transfert dans l'informel comporte de nombreux de risques. Non seulement, il constitue un risque majeur pour la stabilité de la monnaie, mais en cas de problème, la clientèle n'a pas de recours parce que les sociétés exercent dans l'illégalité même si nombre d'entre elles transfèrent de très gros montants à l'international. A cela, il faut ajouter que leurs activités ne sont comptabilisées nulle part et faussent toutes les statiques nationales, voire sous régionales sur la monnaie électronique. En dernier ressort, il constitue un créneau très favorable au blanchiment d'argent. Que faire ? Il s'agit, selon Moussa Diallo, de concevoir une réglementation souple et adaptée, visant à faire évoluer les opérateurs du secteur informel vers le formel, assurer la sécurité des opérations, sauvegarder les intérêts des clients, maîtriser les statistiques et améliorer la fiscalité.

Pour le directeur des moyens de paiement de la BNDA, Oumar Haïdara, le transfert en soi n'est pas un problème pour les banques puisqu'il n'est pas leur vocation première, même si les opérations de transfert leur permettent de bénéficier de commissions et de fidéliser les clients. Un autre spécialiste tire la sonnette d'alarme. « En plus du transfert, certains d'entre eux essaient de faire autre chose. Concrètement, ils cherchent à transformer leurs comptes téléphoniques en comptes bancaires, afin que les clients puissent déposer leur argent et viennent le retirer quand ils veulent. Ce n'est pas légal. Le comble, c'est que personne ne peut contrôler aujourd'hui ce que font en réalité ces opérateurs. Il semblerait que si on leur demande de garantir un milliard, cela trouve qu'ils ont déjà fait le double ou le triple. La monnaie électronique est garantie par une banque et normalement, la banque doit être régulièrement informée par l'opérateur de téléphonie mobile, mais il faut avoir des outils pour pouvoir contrôler efficacement ce qui se passe. Et ce n'est pas le cas ». Notre interlocuteur se demande si demain ces opérateurs proposent des crédits ou des comptes rémunérés à leurs clients, qu'adviendra-t-il des banques dont c'est le cœur du métier. Il insiste sur l'importance de bien réguler le secteur. « Toutefois, tant que les opérateurs de téléphonie restent dans l'activité de transfert d'argent, il n'y a pas de problème», assure-t-il.

Selon nos informations, Orange aurait commandé d'installer des guichets automatiques, mais la BCEAO n'aurait pas accepté en lui opposant la réglementation qui ne l'y autorise pas. L'opérateur aurait alors envisagé la création de sa propre banque.
Aussi, certaines sociétés chercheraient actuellement à nouer des partenariats avec les banques, afin que les clients puissent accéder à leurs comptes grâce à des solutions mobiles. Devant cet essor de la monétique, les banques doivent proposer des alternatives et diversifier leurs produits, car si elles s'intéressent plus au transfert, cela leur permettra de fidéliser leurs clients. Entre autres, elles doivent faire preuve d'ouverture d'esprit et évoluer vers un partenariat gagnant – gagnant puisque les opérateurs de téléphonie, en tant que canaux de communication et de distribution, contrairement aux banques, sont présents un peu partout sur le territoire.
Le nouveau contexte impose aussi une relecture des textes du secteur bancaire. Si la circulaire du 21 mai 2015 définit clairement les règles et au niveau du GIM UEMOA, des textes beaucoup plus précis sont en cours d'élaboration et ont été soumis à la BCEAO.
En attendant, les textes existant sont-ils correctement appliqués ? « Dans ce processus, ce sont les banques qui doivent faire remonter l'information au régulateur, c'est-à-dire à la Banque centrale et jouer un rôle de veille. Mais le font-elles ? Même si elles le font, je pense que pour le moment, cela n'est pas encore très bien organisé », estime notre expert.

Une multitude d'acteurs

Au Mali, différentes structures interviennent dans le domaine du transfert électronique d'argent. Ce sont d'abord, les banques, ensuite les opérateurs de téléphonie mobile (Orange et Malitel). En fait, les opérateurs de téléphonie sont plutôt des canaux de distribution, menant leurs activités sous le couvert des banques (BICIM et BIM) qui ont vocation à le faire. « Mais ces canaux ont pris le pas sur les banques qui leur servent de couverture. Et c'est là toute la problématique », explique le président de l'APBEF, Moussa Alassane Diallo.
La troisième catégorie d'acteurs (Lemonway, Wari) représente des sociétés qui ne sont ni des banques ni des opérateurs de téléphonie. Ce sont des établissements agréés par la Banque centrale pour faire du transfert d'argent.
Enfin, il y a de nombreuses personnes dans l'informel qui font du transfert d'argent dans la rue, les quartiers, au grand marché et qui ne sont enregistrées nulle part. Donc ils opèrent dans l'illégalité. C'est le transfert informel qui constitue un risque majeur pour la stabilité de la monnaie.

Liens : http://maliactu.net/mali-paiement-mobile-un-essor-qui-inquiete-les-banques/

SAMIFIN :
Blanchiment d'argent de 120 milliards d'Ariary via mobile banking

L'an dernier, les opérations de transfert d'argent via un téléphone portable au nombre de 3 892 n'ont pas été justifiées au niveau d'une banque primaire.
Faute de cadre réglementaire, les criminels peuvent utiliser facilement le mobile banking pour un blanchiment de capitaux. (Photo d'archives)
Le service de mobile banking devient un moyen de paiement adopté dans le quotidien des Malagasy depuis ces quatre dernières années. En effet, divers services sont offerts

aux utilisateurs via leur téléphone portable. On peut citer, entre autres, le transfert d'argent, le paiement de factures et les opérations d'achats dans les grandes surfaces ou boutiques éparpillées dans toute l'île. Trois opérateurs de téléphonie mobile offrent ces types de service en collaborant respectivement avec trois établissements bancaires à Madagascar. Mais le SAMIFIN ou Service de Renseignements Financiers a détecté des opérations de blanchiment d'argent portant une valeur de plus de 120 milliards d'Ariary via des opérations cash effectuées avec un téléphone portable au cours de l'année 2013.

3 892 opérations cash. Le SAMIFIN évoque que Madagascar ne dispose pas encore de cadre législatif régissant le commerce en ligne dont le paiement via le mobile banking. Cependant, ce nouveau système de paiement constitue un moyen facilement accessible aux criminels pour le blanchiment des capitaux. Les irrégularités signalées par un établissement bancaire au SAMIFIN illustrent la gravité de ce risque de blanchiment d'argent via le paiement mobile. Il faut savoir qu'un opérateur de téléphonie mobile travaillant en collaboration avec une banque primaire à Madagascar possède actuellement un dispositif de vigilance contre le blanchiment d'argent via le mobile banking. Ils ont imposé un seuil réglementaire autorisé pour une opération cash via le téléphone portable, portant une valeur de 10 millions d'Ariary. Au delà de ce seuil, un formulaire doit être établi par le titulaire du compte pour justifier l'origine des fonds. L'an dernier, 3 892 opérations cash n'ont pas été justifiées au niveau de la banque primaire concernée alors que le volume de chaque opération dépasse ce seuil réglementaire de 10 millions d'Ariary, d'après les explications du SAMIFIN. Ce qui revient au montant total des opérations suspectes de blanchiment de capitaux de plus de 120 milliards d'Ariary.

Multiplication d'envois. Notons que d'autres opérateurs n'ont pas ce dispositif de vigilance servant à prévenir les risques de blanchiment de capitaux. Il se peut ainsi que les criminels effectuent des opérations de transfert d'argent d'un gros montant important mais en dessous d'un seuil qui n'éveille pas les soupçons des entités concernées. Par contre, ils multiplient le nombre d'envois par le biais de leur téléphone portable, a-t-on évoqué. Il s'avère ainsi opportun de mettre en place un cadre règlementaire régissant ce système de paiement en mobile banking.

Liens : http://www.xchange-madagascar.com/actualites/index.php/samifin-blanchiment-dargent-de-120-milliards-dariary-via-mobile-banking/

Les deux fronts ouverts par la France contre Google

Le dossier purement fiscal porte sur 2005-2011. Le dossier pénal, lui, vise 2011-2015. Tulipe. C'est le nom de code choisi par le procureur national financier, Eliane Houlette, pour désigner Google à son insu dans l'enquête pour fraude fiscale et blanchiment de fraude fiscale ouverte le 16 juin 2015 et restée secrète jusqu'à la vaste perquisition de la semaine dernière . « *Nous avons, pour assurer une confidentialité parfaite, décidé de ne jamais prononcer le mot Google, et nous avons travaillé ce dossier uniquement hors réseau pendant presque un an* », a-t-elle indiqué ce week-end dans l'émission « Grand rendez-vous » Europe 1-iTélé-Le Monde.

La « tulipe » (l'une des sociétés visées, « *peut-être la société mère* », est immatriculée aux Pays-Bas) a été cueillie mardi dernier par la perquisition à laquelle ont participé

au total 96 personnes : 25 experts en informatique, 6 représentants du Parquet et tous les enquêteurs de l'Office central de lutte contre la corruption et les infractions financières et fiscales (OCLCIFF).

Deuxième étage de la fusée

Cette procédure pénale qui, selon nos informations, porte sur la période 2011-2015, est le deuxième étage de la fusée lancée par la France contre l'américain. Elle est totalement distincte, mais fait suite à la procédure purement fiscale qui a donné lieu à une visite domiciliaire des locaux de la société à Paris par le fisc en 2011, puis à une proposition de redressement portant sur une somme avoisinant les 1,6 milliard d'euros (intérêts et pénalités de retard compris).

Cet autre dossier, sur lequel les deux parties devraient en toute logique entrer en phase de contentieux, porte selon nos sources sur la période 2005-2011. Il vise à déterminer si Google Ireland Ltd disposait alors d'un établissement stable en France et si elle a omis de déclarer une partie de l'activité qu'elle y réalisait. *Il peut exister des ajustements à la marge, mais nous ne sommes pas dans cette logique »*.

Plusieurs téraoctets de documents

Il y a donc bien deux fronts ouverts contre Google : une procédure fiscale et ensuite une procédure pénale, qui si elle porte sur les mêmes faits, ne porte pas sur la même période d'analyse. *« Dans la procédure fiscale, le fisc a constaté que les pratiques de la société pour éluder l'impôt se reproduisaient chaque année*, décrypte un bon connaisseur du dossier. *Il s'est donc demandé si elles perduraient encore aujourd'hui. C'est pour en avoir le coeur net qu'il a transmis l'affaire au Parquet national financier »*, preuve que Bercy sait aussi, quand il le veut, se coordonner avec la justice dans la chasse à la fraude.

Au pénal, Google encourt jusqu'à 10 millions d'euros d'amende pour le volet fraude fiscale de ce dossier. Quant à l'éventuel délit de blanchiment de fraude fiscale, il est puni de 10 ans de prison et 750.000 euros d'amende ou la moitié des sommes blanchies. La peine pénale ne serait cependant pas exclusive, si le délit était avéré, d'un autre redressement.

Le travail de la justice dans le cadre de cette enquête préliminaire s'annonce long et difficile. *« Nous avons amassé beaucoup de données informatiques, je crois qu'il y a plusieurs téraoctets de documents »*, a précisé Eliane Houlette, qui estime que plusieurs mois, voire plusieurs années seront nécessaires pour les exploiter. *« Nous sommes très limités par les moyens matériels. Il nous faudrait des logiciels extrêmement performants qui existent, mais dont nous ne disposons pas »*. Des outils qui, précisément, font la force de Google. Le 30/05

Liens : http://www.lesechos.fr/tech-medias/hightech/021979444337-les-deux-fronts-ouverts-par-la-france-contre-google-2002383.php

Les terroristes se financent sans les établissements internationaux

Depuis la guerre contre Al-Qaida lancée par Washington, les djihadistes ont trouvé des canaux alternatifs.

Le financement du terrorisme se cache dans les paradis fiscaux. Les révélations du *Monde* sur les fraudes fiscales organisées par la banque britannique HSBC ont mis en lumière le mélange des genres entre clients fortunés et personnalités proches d'Al-Qaida. Évaluée à 17.000 milliards de dollars par le FMI, l'évasion fiscale mondiale profite à de riches particuliers ou à des entreprises ainsi qu'à des groupes terroristes.

Dans les années 1980 et 1990, ces derniers usaient des grandes banques internationales pour se financer. La banque pakistanaise BCCI a fait faillite en 1991 après avoir financé pendant vingt ans des activités criminelles comme le blanchiment d'argent de la cocaïne des cartels colombiens. Un business dans lequel HSBC a aussi été épinglé. Oussama Ben Laden détenait, lui, un compte chez la suisse UBS. Après les attentats du 11 septembre 2001, les banques ont été obligées de durcir leurs contrôles antiblanchiment. "Les terroristes se sont rabattus sur des banques plus petites, dans des pays au lourd secret bancaire et à la réglementation laxiste", explique Damien Martinez, cofondateur du Centre d'analyse du terrorisme. Des banques des pays d'Europe de l'Est, comme dans les Balkans, de la Corne de l'Afrique, comme la Somalie, ou du Soudan. Le Kenya et la Tanzanie, ont, en revanche, fait un grand ménage en fermant, ces dernières années, 500 ONG qui servaient de paravent à des organisations terroristes. Ces associations, très poreuses, disposent de beaucoup de cash. Leurs campagnes de dons permettent de collecter facilement de l'argent et de le blanchir dans le système bancaire. "Mais les banques restent identifiées et des services de renseignements peuvent pister les mouvements sur un compte, souligne Damien Martinez. Le pire, c'est quand l'argent du terrorisme sort du système bancaire, car il n'y a alors plus d'outil pour le contrôler."

Daech contrôle son pétrole et ses banques

Des canaux de financements alternatifs ont vu le jour. En Espagne, Al-Qaida avait créé une trentaine de sociétés commerciales dans le BTP pour blanchir de l'argent via leurs comptes. Un réseau aujourd'hui démantelé. Pour éviter des mouvements massifs, trop visibles, les terroristes lèvent leurs fonds en les fractionnant auprès de dizaines ou de centaines d'individus.

Les djihadistes passent aussi par des organismes de transfert d'argent, comme Western Union, appelés hawala au Moyen-Orient, des cartes prépayées, du crédit à la consommation ou du paiement par mobile. Des systèmes beaucoup plus difficiles à pister. L'organisation État islamique utilise quant à elle un mode de financement inédit. "Daech ne capte plus l'argent à l'extérieur, mais il met la main dessus en contrôlant 20 puits de pétrole et 14 banques en Irak et en Syrie, explique Jean-Charles Brisard, expert en terrorisme. Les donations ne pèsent plus que 2 % de ses ressources financières."

Liens : http://www.lejdd.fr/Economie/Marches/Les-terroristes-se-financent-sans-les-etablissements-internationaux-718158