وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ م

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Lutte contre le financement du terrorisme : vers une analyse des signaux faibles

La lutte contre le blanchiment de capitaux est associée à la lutte contre le financement du terrorisme depuis des années mais ce rapprochement est-il réellement pertinent ? Peut-on vraiment considérer que la détection des flux liés au blanchiment de capitaux doit être appréhendée de façon similaire à ceux relatifs au financement du terrorisme ? Les outils de profilage existants possèdent-ils suffisamment de paramètres pour détecter les opérations liées au financement du terrorisme et pour déterminer un possible passage à l'acte ?

Les outils de profilage des comptes bancaires ont été mis en place pour permettre aux établissements bancaires d'identifier les flux financiers atypiques ou anormaux en fonction du profil identifié en amont d'un client. La plupart des outils fonctionnent sur le principe de seuils d'alerte. Les événements récents ont permis de mettre à jour d'autre types de financement que le réseau bancaire classique : utilisation de monnaies virtuelles, recours à des Hawalas (système informel de compensation) ou encore transfert d'espèces via des réseaux du type Moneygram ou Western Union, cartes prépayées. Ces événements ont également confirmé le peu de moyens requis pour passer à l'acte.

Si le financement du terrorisme passe en dessous des seuils d'alerte et si la modification du comportement "classique" n'est pas détectée au titre de l'outil existant, comment prévenir et identifier les auteurs d'actes terroristes ? Comment alors considérer que les outils de profilage bancaire tels qu'ils existent actuellement peuvent permettre d'identifier des flux liés au financement du terrorisme si ces flux ne passent pas ou très peu par des comptes bancaires classiques et si les montants ne sont pas significatifs au regard des seuils d'alerte implémentés ?

Nous proposons de faire évoluer ces outils pour leur permettre de détecter des signaux faibles. Ces évolutions ne sont évidemment pas sans conséquences pour les établissements bancaires utilisateurs. Cependant ces évolutions peuvent à notre sens dépasser largement le cadre stricte du terrorisme.

L'utilisation des outils existants pour détecter les signaux faibles

Un « signal faible » peut être vu comme un « outil » d'aide à la décision. Il se présente généralement comme une « donnée » d'apparence anodine mais dont l'interprétation que l'on en fait peut déclencher une alerte. Cette alerte indique que pourrait survenir un événement susceptible d'avoir des conséquences considérables (en termes d'opportunité, de menace ou de risque). Après interprétation le signal n'est d'ailleurs plus qualifié de faible, mais de signal d'alerte précoce.

Quels sont les signaux faibles à détecter dans le cadre du terrorisme ? L'absence de flux, la baisse de flux ou encore le changement de comportement dans l'utilisation des moyens de paiement devraient être autant d'indices pouvant mériter une investigation approfondie.

En effet, tout passage à l'acte nécessite une phase de préparation et c'est cette phase de préparation qui à notre sens pourrait être décelée par les outils de profilage. Par exemple, une personne se radicalise, son nouveau mode de vie peut passer inaperçu aux yeux de sa famille. Cependant son mode de consommation va nécessairement se modifier.

Les signaux faibles qui pourraient être détectés et analysés : la suppression des abonnements téléphoniques classiques, la baisse de l'utilisation de la carte bleue ou encore la baisse de flux de consommation normale etc.

Cependant, le problème de détection est à la mesure de l'enjeu et des difficultés de détection des actes de terrorisme et de leur financement ? Comment permettre aux outils de profilage de détecter ces signaux faibles mais aussi comment permettre aux établissements bancaires de traiter ces alertes d'une façon sereine ?

L'évolution nécessaire des outils de profilage

À notre sens le profilage bancaire trouve ses limites et sa force dans l'absence de flux. Les limites sont clairement identifiables : pas ou peu de petit flux n'entraînent pas d'alerte donc difficulté à déterminer en amont les comportements anormaux ou les changements de comportement d'un individu pouvant passer à l'acte. Il convient à notre sens de paramétrer et de repenser les outils de profilage pour leur permettre d'évoluer vers la détection de signaux faibles.

La conséquence non négligeable de ce recalibrage sera la nécessaire hausse des alertes à traiter. Cela peut effectivement constituer un frein à la mise en place de ces nouveaux procédés. Cependant les établissements bancaires et financiers devront faire un arbitrage entre le coût et les risques. N'est-il pas plus impactant de ne rien mettre en place en termes d'image, de potentielle sanction que d'affiner les paramètres d'un outil et de recruter plus de ressources pour traiter les alertes ?

Cet arbitrage entre coût et risques doit également à notre sens se faire en analysant les autres apports de ces évolutions.

La détection des signaux faibles au service du blanchiment de capitaux, de la lutte contre les fraudes et du développement commercial

En effet, accentuer la détection des changements de comportement d'un client par le développement des outils de profilage ne servira bien sûr pas uniquement la lutte contre le terrorisme. Elle permettra de rendre plus pertinente les alertes liées au blanchiment de capitaux. Elle permettra également d'utiliser cet outil dans la détection des fraudes externes. Prenons un exemple concret, si un client utilise des moyens de paiements qu'il n'utilisait pas avant, en démarrant une investigation via ces nouvelles alertes, il sera possible de se rendre compte que son chéquier est utilisé par une autre personne.

Enfin cet outil pourrait également servir d'outil de développement commercial ; en effet, mieux comprendre le comportement de son client permet d'adapter les services que les établissements peuvent lui proposer.

En conclusion, l'évolution des outils de détection nous paraît nécessaire pour s'adapter aux nouveaux enjeux liés au terrorisme. Cette évolution représente un coût mais ce coût peut être atténué par l'utilisation de ces évolutions pour d'autres problématiques comme la lutte contre les fraudes ou le développement commercial.

12.01.2016

Liens : http://bankobserver.solucom.fr/lutte-contre-le-financement-du-terrorisme-vers-une-analyse-des-signaux-faibles/

Pour le Trésor américain, Le groupe EI a de gros soucis financiers

D'après un haut responsable du Trésor américain qui s'est exprimé hier jeudi, le groupe État islamique (EI) a des soucis financiers. Il peine à payer ses combattants et a dû imposer de nouvelles taxes pour compenser les pertes liées aux bombardements de la coalition internationale.

"Quand nous recevons des indications que l'EI ne peut pas payer les salaires de ses propres combattants et tente de compenser par d'autres sources de revenus, nous savons que nous les frappons là où ça fait mal", a affirmé Daniel Glaser, secrétaire adjoint en charge de la lutte contre le financement du terrorisme. Les bombardements menés depuis août 2014 sous supervision américaine "perturbent" la production des champs de pétrole dont l'EI s'est emparé en Irak et dont il a tiré "500 millions de dollars" en 2015, soit la moitié de ses revenus totaux, selon les déclarations de M. Glaser.

"Même si c'est difficile à quantifier, les frappes ont sans aucun doute limité la capacité de l'EI à produire et vendre du pétrole et à en retirer des bénéfices comme par le passé", a déclaré le responsable lors d'une audition devant une commission du Congrès. De récentes frappes aériennes ont également visé des réserves de caches d'argent liquide, privant l'EI de plus de 100 millions de dollars de ressources, a-t-il ajouté.

Pour compenser le manque à gagner, le groupe jihadiste qui contrôle de larges pans des territoires syrien et irakien a commencé en février dernier à imposer des taxes sur les populations les plus pauvres, qui en étaient jusque-là exemptées, et a de plus recours à "l'extorsion" pour financer ses opérations, affirme M. Glaser.

Une étude publiée mi-avril par le cabinet spécialisé IHS Jane's dessinait la même tendance en affirmant que les revenus du groupe jihadiste avaient fondu d'environ 30% depuis l'an dernier. 10/06/2016

Liens : http://www.boursorama.com/actualites/pour-le-tresor-americain-le-groupe-ei-a-de-gros-soucis-financiers-c33afae2694611ae91c0129c825bc016

Arnaque Western Union : Les différents scénarios possibles

L'arnaque Western Union ainsi que d'autres arnaques de ce type et provenant de Côte d'Ivoire sont très nombreuses, et même en augmentation ces derniers mois. Si vous avez déjà vécu ce genre d'arnaques, vous aviez probablement eu affaire à l'une citées dans cet article.

L'arnaque au client mystère (Secret Shopper)

Vous êtes contacté soudainement (souvent en anglais ou dans un français catastrophique) par un individu qui vous propose de faire une mission en tant que « client mystère ». Vous recevez des « *traveller chèques* » (chèques de voyage) d'un montant important avoisinant généralement le millier d'euros et quelques semaines

plus tard, vous apprenez qu'ils ont été refusés par votre banque car ils ont été contrefaits ou volés.
Entre temps, vous avez bien entendu reversé une rémunération de quelques centaines d'euros et viré le montant restant à une personne X ou Y. Ce montant, vous ne le reverrez jamais en plus de ne pas recevoir votre rémunération… Dans ce cas là, il est primordial de prendre contact avec la société émettrice des travellers chèques afin de vérifier le numéro de série, cela prend 5 minutes et vous pourrez les jeter à la poubelle directement sans vous faire arnaquer.

L'arnaque aux sentiments

Les cyber-escrocs créent des faux comptes sur des sites de rencontre, ou sur les réseaux sociaux en utilisant des photos d'hommes ou de femmes récupérées sur internet. Leur but est d'entretenir pendant des semaines voir des mois des conversations sentimentales avec des internautes.
Les cibles sont souvent choisies, c'est-à-dire des personnes qui sont déjà affaiblies sentimentalement au moment de la rencontre. À un moment donné, ils solliciteront leur victime pour l'achat d'un billet d'avion leur permettant de leur rendre visite, pour l'achat de quelques nuitées à l'hôtel, pour aider un proche tombé soudainement malade ou victime d'un accident, etc. Les raisons ne manquent pas, les seules limites sont la capacité d'imagination de l'escroc !
Ces arnaqueurs qui se font appeler « *brouteurs* » en Côte d'Ivoire maîtrisent très bien la langue française ainsi que les outils informatiques, dont les logiciels webcam truqués et de retouches d'images. Les excuses données par la suite sont très bancales, on apprend qu'ils se sont fait arrêter à l'aéroport car leurs vaccinations n'étaient pas à jour, ou car un autre phénomène « imprévisible » est arrivé. Dans ce cas, il n'y a que la vivacité d'esprit et la perspicacité qui peut empêcher de tomber dans le panneau. Ne pas être trop crédule, surtout sur le Net avec des total inconnus.

L'arnaque à l'héritage

Il s'agit en général de prétendus fonds (des dizaines de milliers d'euros) qui se trouveraient bloqués dans une certaine banque au nom d'un certain héritier ne pouvant récupérer son avoir sans l'intervention d'un tiers. Les escrocs manient là encore très bien la langue française et font douter les internautes en utilisant des noms réels et des adresses mail qui semblent légitimes.
Les escrocs récupèrent ensuite vos coordonnées bancaires ou vous font payer plusieurs « frais de dossier » ou douaniers en cascade. Les motifs donnés sont très variés, il peut s'agir d'une personne atteinte d'une grave maladie ou décédée, d'un objet qui n'a pas pu être livré, etc. Avec une simple recherche Google sur le mail de l'escroc, vous tombez généralement sur des résultats probants.

Les arnaques Le Bon Coin

Ces arnaques prennent plusieurs formes mais ont habituellement toutes un point commun : une offre excessivement alléchante. Certains escrocs répondent à vos annonces en indiquant être un acheteur résidant en Côte d'Ivoire. Ils demandent l'expédition de votre objet (souvent de véhicules) depuis la France à vos frais avec promesse de règlement dès réception, ou en demandant vos coordonnées bancaires pour un prétendu « paiement ».
D'autres escrocs vendaient sur Le Bon Coin des objets en demandant un paiement par mandat-cash, bien-sûr les acheteurs ne recevaient jamais leur commande. Faîtes également attention avec votre numéro de téléphone, lorsque vous initiez une conversation de ce type, vous risque d'être inondé d'appels et de SMS toute la journée!

L'arnaque à la loterie

L'une des plus populaires, et sûrement l'une des moins efficaces à présent. Les mails finissent en grande majorité dans les dossiers spam et ne sont pas convaincants. L'un des derniers en date était plutôt marrant, à savoir une "Loterie Microsoft" accompagnée de photos de Bill Gates, vous annonçant que vous êtes l'heureux gagnant de plusieurs dizaines de milliers d'euros. Fake !

L'arnaque Skype (anciennement MSN)

Votre contact réel se fait pirater et l'escroc se sert du compte pour demander de l'aide, notamment pour l'achat d'un objet ou le paiement d'un loyer.

L'arnaque au remboursement

Pour vous faire croire que l'on va vous aider, on vous propose des faux sites et fausses adresses mail à contacter, tout en cherchant à vous arnaquer une deuxième fois.

Ne croyez absolument pas les sites qui vous proposent de vous aider ou de vous rembourser, pareil pour les adresses mail du type « interpole-service-anti-arnaque@hotmail.etc ». A noter qu'il y a eu plusieurs commentaires de ce type postés sur UnderNews depuis un an, la plupart modérés.

Les seules vraies adresses et sites se trouvent à la fin de cet article.

D'autres arnaques plus techniques

Le phishing ou hameçonnage, vous recevez un mail provenant soi-disant de *PayPal* ou de votre banque vous demandant de mettre à jour vos informations. Plus dangereux encore, un faux mail de paiement PayPal en réponse à la vente d'un objet en ligne sur un site de petites annonces : vous envoyez alors l'objet en pensant avoir été payé mais il n'en ai rien ! Pensez à vérifier systématiquement dans votre compte PayPal que la somme a bien été véritablement versée (ne surtout pas accorder de l'importance aux mails reçus).

Cette arnaque est très utilisée sur Le Bon Coin ou eBay et fait énormément de victimes en France. Un reportage au journal de 20H a d'ailleurs été diffusé juste après les fêtes pour avertir des risques.

Et le pire dans tout ça ?

Beaucoup de victimes arnaquées ne portent pas plainte, car elles se sentent embarrassées d'être tombées dans le piège.

Celles qui portent plainte ne revoient tout de même pas leur argent ou objet car la police française ne prend pas souvent (jamais ?) le temps de faire les démarches. Les escrocs se trouvent à l'étranger et sont, pour la plupart du temps, intouchables.

Comment éviter ces arnaques ?

Ne faîtes d'une manière générale absolument pas confiance aux annonces de ce type, et restez vigilent et informés. Ne répondez pas aux mails lorsqu'ils sont alléchants ou vous demandent vos identifiants et/ou informations bancaires.

Utilisez TinEye sur les images des réseaux sociaux et annonces pour savoir si l'image a été récupérée sur Internet ou non

Liens : https://www.undernews.fr/reseau-securite/arnaque-western-union-les-differents-scenarios-possibles.html

Au tribunal de l'Internet : Une société sans pièces ni billets est-elle réaliste ?

Rendue possible grâce aux technologies, une société sans cash est-elle pour autant une bonne idée ? À vous de juger !

Le meilleur des mondes est-il un monde sans cash ? Certains économistes prédisent que, dans une dizaine d'années, nos porte-monnaie disparaîtront, faute d'argent liquide à y stocker. Des pays comme Suède et la Norvège sont déjà très en avance sur la voie des paiements dématérialisés, misant sur le développement exponentiel du paiement sans contact par carte et téléphone mobile. Et les fabricants rivalisent d'imagination sur ce marché prometteur. Google, par exemple, expérimente son nouveau service *Hands free* qui évite au client de sortir son téléphone de sa poche. Il suffit de dire au caissier « Je paye avec Google », de lui communiquer ses initiales et sa photo préenregistrée, et le paiement se réalise via les technologies Wifi et Bluetooth.
Les adeptes d'une société sans pièces ni billets vantent ses multiples avantages, à commencer par la simplicité et la rapidité des transactions. Faute d'avoir à sortir sa carte et à taper son mot de passe, le consommateur est protégé contre le risque d'usurpation de ses données bancaires. En outre, la traçabilité des opérations empêchera le blanchiment d'argent, l'évasion fiscale et le travail dissimulé. La dématérialisation des paiements est, en revanche, un terrain propice aux cyberattaques visant les terminaux de paiement et les serveurs. Et d'ailleurs, en Suède, les fraudes aux paiements électroniques ont été multipliées par deux en 10 ans.

Verrouillage étatique ?

Par ailleurs, du point de vue des libertés, est-il prudent de confier son patrimoine financier à des machines ? Certains experts en doutent, pressentant l'asservissement des individus à une sorte de dictature orwellienne : « La société sans cash qu'on nous promet grâce au numérique donnerait aux décideurs – sans possibilité d'échappatoire pour les particuliers, faute d'avoir assez d'argent liquide – les moyens de contrôler tout le système : pensons au verrouillage des retraits de cash en Grèce », avance le professeur d'économie Henri Bourguinat dans une tribune publiée par le journal *Le Monde* en mars 2016.
La fin de l'argent liquide est-elle une bonne idée ? À vous de juger ! Mais après avoir regardé le 43e épisode de la série Au tribunal de l'Internet ! dans lequel nos deux expertes, Myriam Quemener et Christiane Féral-Schuhl, plaident le « pour » et le « contre » en... trois minutes ! 23/05/2016

Liens : http://www.lepoint.fr/justice-internet/au-tribunal-de-l-internet-une-societe-sans-pieces-ni-billets-est-elle-realiste-23-05-2016-2041285_2081.php

Trois mafieux du gang des vélos de luxe arrêtés en Moldavie

Pour eux, la France c'était « le pays des fleurs et du miel ». Un terrain de chasse grandeur nature où florissait leur incroyable business de vélos de luxe. De 2014 à 2015, un gang de la sulfureuse mafia Vory v Zakone s'était enrichi d'un million d'euros en menant 57 raids dans des magasins de cycles de région parisienne mais aussi de province. Mais cette fois, il y a quelques jours, c'est une autre image de la France que les membres du gang ont eue en voyant débarquer chez eux, en Moldavie, des policiers de la sûreté départementale du Val-de-Marne accompagnés de leurs homologues locaux.
Dans leurs mains, pas de fleurs ni de miel mais une commission rogatoire internationale. Une opération exceptionnelle, menée avec l'office central de lutte contre la délinquance itinérante, hors de l'espace Schengen dans un pays de l'ex-URSS. Le bilan : 24 perquisitions en quatre jours dans six villes de Moldavie et trois membres de la mafia arrêtés. Et parmi eux, un donneur d'ordres qui avait pris soin de changer d'identité en prenant le nom de sa femme, un lieutenant chargé de valider les

opérations, et un spécialiste qui avait pour mission de blanchir l'argent sale grâce à des entreprises de viande du pays.
Les opérations étaient à chaque fois menées tels des commandos. Le premier date de juin 2014 à Bonneuil-sur-Marne (Val-de-Marne) dans un magasin de cycles. Une nuit, à l'aide d'une disqueuse, les monte-en-l'air de l'équipe découpent une partie du toit pour accéder au commerce. Il ne leur reste plus qu'à remonter les vélos, d'une valeur de 4 000 à 15 000 €, à l'aide d'un grappin. A chaque cambriole, une vingtaine voire une trentaine de cycles s'évanouissent par les airs.
Deuxième étape de la course : le retour au pays. Les vélos sont démontés et disposés dans des minibus. Pour éviter d'être repérés par la vidéosurveillance des stations-service, les convoyeurs prennent soin auparavant de cacher des jerricans d'essence en rase campagne sur le parcours.
Dernière étape : la revente. « C'est plus facile de refourguer des vélos plutôt que des voitures car il n'y a pas de numéro de série, précise un policier. Ils étaient sans doute revendus en ligne via des sites d'hébergement moldaves ou des pays de l'Est ».
La première vague d'interpellations date de septembre dernier quand treize membres du gang se trouvaient encore en France. « Mais il en manquait. Alors on est allés les chercher en Moldavie pour bien leur faire comprendre qu'on ne les lâche pas », savoure un enquêteur. Interrogés, les gangsters sont restés muets ou ont donné des explications fantaisistes. « La mafia Vory v Zakone, au code d'honneur strict et dont les membres sont reconnaissables à leurs tatouages, est ultra-violente. Pour les membres qui font preuve de déloyauté, la réponse est sanglante », souffle un policier. Reste aujourd'hui à obtenir l'extradition des gangsters. Pour un retour pas vraiment bucolique au pays des fleurs et du miel. 12 mai
Liens : http://www.leparisien.fr/bonneuil-sur-marne-94380/trois-mafieux-du-gang-des-velos-de-luxe-arretes-en-moldavie-12-05-2016-5789819.php

Escroquerie au CO2:
Les nouveaux braqueurs s'attaquent au fisc

Ils achetaient du "droit à polluer" à l'étranger puis le revendaient en France, gardant au passage la TVA correspondante: les braqueurs de l'escroquerie au CO2 sont jugés à partir de ce lundi à Paris.
Ces rois de l'escroquerie financière, dont certains sont jugés ce lundi, soustraient chaque année des millions d'euros au fisc et aux entreprises. Enquête sur des casseurs en col blanc qui ont noué d'étroites relations avec le grand banditisme.
Ils n'attaquent pas les fourgons de transport de fonds, ne forcent pas les coffres-forts. Ils ne brandissent pas de gros calibres, ne travaillent pas à l'explosif. Leurs forfaits ne font pas couler le sang de leurs victimes. Ces braqueurs-là agissent dans l'ombre, armés de leur téléphone, de leur ordinateur et de leur "déballe" [NDLR: leur tchatche].

Leur spécialité, ce sont les arnaques financières - les belles, les grandes, celles qui se chiffrent en millions d'euros et promènent les enquêteurs de prête-noms en sociétés écrans, de comptes bancaires exotiques en para dis fiscaux. Car ces amateurs de palaces et de yachts, de filles et de tapis vert connaissent sur le bout des doigts les règles de la finance, les arcanes de la législation et les us et coutumes des entreprises.
Les policiers les appellent le "milieu affairiste franco-israélien". Eux disent "les feujs" ou "les juifs", tout simplement. "Cela représente 40 à 60 personnes, très astucieuses et opportunistes, qui se trouvent aujourd'hui au coeur de la criminalité française", précise

un spécialiste. Leurs mauvaises fréquentations préoccupent le Sirasco, le service de renseignement de la police judiciaire: selon son dernier rapport annuel, "plusieurs enquêtes ont pu démontrer que ces escrocs s'étaient associés à des organisations criminelles du grand banditisme traditionnel". Entre les fraudes à la TVA et les virements soutirés aux entreprises, le montant de leur butin donne le vertige: plus de 2 milliards d'euros sur les huit dernières années.
Le casse du siècle, c'est eux: une monumentale arnaque à la TVA sur le marché européen des droits d'émission de dioxyde de carbone (CO2), qui aurait coûté 1,6 milliard d'euros au fisc français, d'après les estimations de la Cour des comptes, entre l'automne 2008 et la fin du printemps 2009. "Le CO2, c'était *Alice au pays des merveilles*", soupire l'un de ces "affairistes", des étoiles dans les yeux.
Résumons. Pour diminuer les émissions de gaz à effet de serre, les Etats ont fixé aux usines les plus polluantes un plafond annuel de rejets de CO2. Si les entreprises dépassent leurs quotas, elles doivent acheter des "droits à polluer". Si, à l'inverse, elles ne les épuisent pas, libre à elles de les revendre. Les fraudeurs ont vite détecté la faille: il suffit d'acheter, hors taxe, des quotas de CO2 dans un pays, puis de les revendre aussitôt dans un autre, taxe comprise cette fois... Sans reverser la TVA à l'Etat. Si fournisseur et client sont de mèche, l'opération peut être répétée. Un tel "carrousel de TVA", selon l'expression consacrée, rapporte 19,6% à chaque tour de manège. Le septième ciel pour les princes de la "tève".

Adepte des sacs en croco

Quatre d'entre eux seront à l'affiche du tribunal correctionnel de Paris à partir du 2 mai prochain, dans deux dossiers distincts. Mardoché Mouly, dit "Marco l'élégant", et Arnaud Mimran, le flambeur des beaux quartiers, sont accusés, avec dix comparses, d'avoir monté un hold-up à 283 millions d'euros sur le marché des fameux droits à polluer. Cyril Astruc, l'habile financier adepte des sacs en croco, et le Lyonnais Stéphane Alzraa, collectionneur de berlines de luxe, sont impliqués, eux, dans l'affaire Michel Neyret, ce grand flic lyonnais soupçonné de relations troubles avec quelques figures du milieu, sur fond de séjours au soleil et de petits cadeaux.
Mouly, Mimran, Astruc et Alzraa. Ces hommes sont de vieilles connaissances. "Chez les 'affairistes', on fait du business les uns avec les autres, expli que un observateur averti. Certains ont même grandi ensemble, à Belleville, comme les Mouly, les Touil et les Souied, trois des grandes familles de ce milieu." Dans ce petit monde qui vénère l'argent et révère la famille, on travaille entre frères, cousins et amis, on célèbre ensemble mariages et bar-mitsva, on se brouille (souvent), on se vole (parfois), mais on se réconcilie (presque toujours).
Beaucoup ont fait leurs premières armes dans le textile ou dans les encarts publicitaires, cette escroquerie qui consiste à vendre, très cher, des espaces de pub dans des revues professionnelles ou dans des annuaires en ligne, parfois fictifs, à de petits commerçants et artisans. "Patrick Souied, aujourd'hui décédé, faisait figure de pionnier du genre, mais l'as des as, c'était Cyril Mouly, le cousin de Marco, raconte un homme qui les connaît bien. Quand un coup menaçait de foirer, on l'envoyait, lui."
Mais la baraka finit par abandonner le "Frenchman", son surnom autour des tables de poker. Extradé du Maroc où il s'est réfugié, le quadragénaire à la tignasse poivre et sel est condamné à cinq ans de prison par le tribunal correctionnel de Bordeaux, en 2014, pour avoir soutiré 15 millions d'euros à une dizaine d'entreprises.

Le faux président, le faux bailleur...

Très doué, lui aussi, en "déballe", Gilbert Chikli a peaufiné un redoutable scénario pour duper les entreprises. En juillet 2005, il appelle la directrice d'une agence postale parisienne. Se présentant comme le patron de La Poste, il l'avertit qu'un agent des

services secrets va la contacter dans le cadre d'une opération de lutte contre le blanchiment d'argent. Bien sûr, elle devra suivre à la lettre ses instructions. Bingo: la jeune femme dépose 358000 euros dans les toilettes d'un bar, place de la Nation. En l'espace de 18 mois, 33 sociétés sont ciblées, parmi lesquelles les banques HSBC et Barclays, le groupe de transport Alstom et le géant mondial du conseil Accenture.
Chikli et ses comparses, dont ses frères Thierry et Simon, ne font pas mouche à tous les coups, certes, mais ils détournent tout de même 7,9 millions d'euros. En mai 2015, quand la justice lui inflige sept ans d'emprisonnement, l'oiseau s'est déjà envolé. Réfugié en Israël depuis six ans, il vit dans la station balnéaire d'Ashdod, sous l'oeil des 30 camé ras de surveillance qui truffent sa villa. Il y reçoit volontiers des journalistes, auxquels il montre les impacts de balle sur le mur d'enceinte.
Le petit gars de Belleville a fait école. Ses émules ont multiplié les variantes: après le faux président, le faux bailleur (l'escroc se fait passer pour le propriétaire des locaux de l'entreprise et prétend avoir changé de banque) ou le faux changement de RIB (dans ce cas, c'est un fournisseur qui affirme avoir un nouveau compte bancaire).
"Les aigrefins sont très méticuleux: ils rassemblent toutes les données disponibles sur l'entreprise, via Internet ou le registre du commerce, voire en utilisant des logiciels espions, souligne la commissaire divisionnaire Corinne Bertoux, à la tête de l'Office central pour la répression de la grande délinquance financière (OCRGDF). Et pour mettre en confiance le salarié contacté, ils écument les réseaux sociaux à la recherche d'informations personnelles."
Les deux tiers des sociétés françaises auraient déjà subi une attaque de ce type. Tous les mois, malgré les alertes de la police et des organisations patronales, elles sont des dizaines à tomber dans le panneau. Inter marché, au printemps dernier, a été délesté en quelques jours de... 15 millions d'euros. Même les clubs de foot sont visés: à l'automne 2014, l'Olympique de Marseille a viré 756000 euros à deux Franco-Israéliens, croyant rémunérer l'avocat d'un joueur. A ce jour, 2300 entreprises ont porté plainte, pour un préjudice cumulé de 485 millions d'euros. "Sans compter toutes celles qui préfèrent se taire, plutôt que risquer une publicité négative", pointe un bon connaisseur du sujet.

Le plus joli coup: le CO2

L'autre royaume des "affairistes", c'est la fraude à la TVA. Une arnaque vieille comme cet impôt instauré en 1954, mais constamment adaptée aux nouveaux marchés, aux nouvelles opportunités. "Il y a eu des modes, détaille un expert: les téléphones, les composants électroniques, le platine, le cuivre... Aujourd'hui, c'est plutôt le gaz, les installations photovoltaïques, les terres rares et la fiscalité écologique." Chaque année, 14 milliards d'euros de TVA s'évaporent en France.
Le plus joli coup des pros de la "tève" reste le CO2. "C'est comme si vous laissiez une Ferrari à La Courneuve avec les clefs dessus", tentera d'expliquer un tradeur lors de son procès. En mieux: pas de risque de vol avec les droits à polluer; pas de coût de transport; des clients à la pelle, puisque les Etats ont créé des Bourses du carbone pour rapprocher l'offre et la demande. Cerise sur le gâteau, la place française, baptisée BlueNext, règle la TVA, rubis sur l'ongle, aux vendeurs.
Une fois la brèche repérée, les aigre fins la prennent d'assaut. En juin 2009, quand Bercy se décide enfin à supprimer la taxe sur ces échanges, ils ont accumulé un magot de 1,6 milliard d'euros. Et poursuivent leur juteux business dans les pays qui n'ont pas encore imité la France - la Belgique, l'Italie et l'Allemagne, notamment.
Flambeurs et hâbleurs, les spécialistes du CO2 font des envieux parmi les bandits endurcis. Quel investissement, en effet, permet à la fois de blanchir de l'argent sale, tout en rapportant environ 14% net à chaque tour de carrousel, une fois déduits les

frais bancaires et le pourcentage du courtier? "Pour se protéger et, parfois, pour récupérer leurs gains, ils ont eu besoin de se rapprocher des voyous. Lesquels ont flairé le bon coup financier", résume un policier.
"Affairistes" franco-israéliens et criminels du milieu nouent des liens étroits. En témoigne une conversation enregistrée le 21 février 2013, au bar du luxueux hôtel George-V, à Paris. Face à face, Grégory Zaoui et Mickaël Ettori, membre de la bande ajaccienne du Petit Bar, soupçonnée de trafic de stupéfiants et d'extorsion. "Vous, hormis le besoin que vous avez comme tout le monde de faire de l'argent, vous avez surtout le besoin de blanchiment [...], lâche Zaoui à son interlocuteur. Nous, on sait faire."
Autre indice de ces liaisons dangereuses: lors d'une perquisition chez Arnaud Mimran, les enquêteurs ont mis la main sur la photocopie de la carte d'identité et du permis de conduire de Mario Hornec, l'un des piliers de ce clan familial gitan, fiché au grand banditisme. Un hasard, selon Mimran: Mario Hornec aurait conduit l'une de ses voitures prêtée à un ami.
En France, dès 2009, les douanes judiciaires se lancent aux trousses des escrocs de la "Carbon Connection", décryptant leurs transactions téléphoniques et détricotant l'écheveau de leurs comptes offshore et de leurs sociétés écrans. "Ils sont très malins, reconnaît un policier de l'OCRGDF. Les auditions et les gardes à vue, avec eux, ressemblent à des parties de poker, ce jeu qu'ils adorent. Et ils nous font bien marrer..."

Les quatre cadavres

Mais l'heure n'est plus à la rigolade. Le jackpot du CO2 a chamboulé le petit monde des fraudeurs. Ces dernières années, on a relevé quatre cadavres dans leur entourage. Amar Azzoug, réputé proche du milieu corso-marseillais, est abattu, en avril 2010, dans une brasserie de Saint-Mandé (Val-de-Marne). Avec lui se trouve Patrick Bellaiche, qui comparaîtra en mai prochain aux côtés de Marco Mouly et d'Arnaud Mimran. L'un de leurs associés, Samy Souied, tombe cinq mois plus tard, criblé de balles, porte Maillot, à Paris. Mimran et Mouly sont présents ce soir-là.
En octobre 2011, c'est le milliardaire Claude Dray, ancien beau-père de Mimran, qui est assassiné dans son hôtel particulier de Neuilly-sur-Seine. La dernière victime en date s'appelle Albert Taieb. L'homme à tout faire de Cédric Mouly, le cousin de Marco, est poignardé à mort dans le XVIIe arrondissement, en avril 2014. Commentaire désabusé d'un roi de la TVA: "Et dire qu'en dix ans de carrousels de TVA dans la téléphonie on n'avait pas connu une seule embrouille..."
Aujourd'hui, la justice les rattrape. Le 30 mars prochain, un mois avant le procès du tandem Mouly-Mimran, débutera celui de Mickaël Kolkowicz, alias "le petit Kolko", qui aurait empoché 2 millions d'euros en huit jours. Quinze dossiers de fraude au CO2 sont ouverts au parquet national financier, une poignée d'autres à Lyon.
Plusieurs "pointures" du milieu affairiste sont visées: les incontournables Stéphane Alzraa et Cyril Astruc; Grégory Zaoui, l'un des précurseurs du CO2; Yannick Dacheville, condamné en mai 2014 à douze ans de prison dans une affaire de stupéfiants; la Marseillaise Christiane Melgrani, qui, murmure-t-on, aurait conçu la martingale. A lui seul, le volet phocéen de cette entourloupe sans précédent aurait coûté 380 millions d'euros au fisc...
Pas sûr, pourtant, que le Trésor public récupère un jour les millions envolés. "Identifier les biens des cadors de la 'tève' est extrêmement difficile, car ils dissimulent leur patrimoine derrière des sociétés immatriculées dans les paradis fiscaux", constate un enquêteur, pessimiste. Pas sûr, non plus, que les "affairistes" passent beaucoup de temps derrière les barreaux.

Dès que le ciel judiciaire devient menaçant, ils ont la fâcheuse habitude de prendre la poudre d'escampette, direction Israël. Comme Fabrice Sakoun et Michel Keslassy, les deux seuls condamnés du CO2 à ce jour, et Gilbert Chikli. Comme, semble-t-il, Stéphane Alzraa, en fuite depuis quatre mois. Là-bas, le business continue. Jamais en panne d'imagination, quelques Franco-Israéliens ont déjà concocté une nouvelle arnaque 2.0: des sites de trading qui promettent le pactole aux internautes prêts à jouer leurs économies sur l'évolution du dollar, du baril de pétrole ou du lingot d'or. 25/03/2016 .

Liens : http://www.lexpress.fr/actualite/societe/les-nouveaux-braqueurs-s-attaquent-au-fisc-et-aux-entreprises_1775957.html

L'argent sale transformé en montres et voitures de luxe

Les services américains et français ont démantelé un réseau de blanchiment de l'argent de la drogue de Colombie, via un système de commerce de montres et de voitures de luxe destinées au Liban.

Il est 20 heures, ce 20 janvier au soir. Ali Z. est attablé dans un palace de l'avenue George-V, lorsqu'on vient discrètement le prévenir qu'il est demandé. Le début de quatre-vingt-seize heures de garde à vue. Quelques minutes plus tôt, à leur arrivée à Roissy en provenance de Beyrouth, c'est l'interpellation de M. E. et M. N. qui a lancé le top départ d'un vaste coup de filet à travers l'Europe. Les policiers de l'OCRGDF (Office central de lutte contre la grande délinquance financière) finalisent un an d'une enquête au cours de laquelle ces deux hommes sont apparus comme les coordinateurs d'un tentaculaire réseau de blanchiment.

Des billets dans les sacs de sport

Décembre 2012 : un passeur est arrêté en France avec 390 000 €. En novembre et décembre 2014, deux autres sont appréhendés en Hollande avec respectivement deux millions puis 500 000 €, en marge d'une saisie de 62 kg de cocaïne. Aux Etats-Unis, les agents de la DEA en ont la certitude : tous appartiennent à une seule et même organisation, pilotée conjointement depuis la Colombie et le Liban, avec la France comme plaque tournante.

L'OCRGDF est saisi. Une à une, courant 2015, les petites mains sont identifiées. Il y a K. actif en Allemagne, quand son homologue J. se charge de l'Italie, voire de l'Espagne. J. se vante d'avoir trouvé une cache infaillible, sous les essuie-glaces de son Land Rover. Aux ordres de M. basé au Liban, c'est H.T. qui chapeaute le réseau en Europe, et se charge parfois lui-même de rapatrier l'argent de la drogue en France et en Allemagne. L'occasion de se rendre compte des difficultés rencontrées par ses subordonnés. Ainsi renâcle-t-il lorsqu'il découvre, arrivé en Italie, que la somme qu'un certain « G. » doit lui remettre atteint 600 000 EUR en coupures de 20.

« On n'en veut pas ! », tranche M. au téléphone, les deux hommes étant sur écoute. « Tu ne savais pas ce que c'était avant ? » s'agace H. « Si je le savais, tu crois que je t'aurais envoyé ? s'excuse son boss. Dans un premier temps, c'était 400. Ils sont devenus 600... » Par sécurité, des « token » — sortes de mots de passe — sont utilisés. Le système consiste à se munir d'un billet de 5 € présenté au collecteur. Il en a reçu au préalable le numéro de série, ce qui permet de s'assurer qu'il est bien celui qu'il prétend être. Au téléphone aussi, tout le monde parle en langage codé. On va ainsi au « four » ou au « moulin », soit en Belgique ou en Hollande. Les montants collectés deviennent, oralement, des modèles de voiture. Une « S500 » doit ainsi être récupérée

à Naples, selon M. « Quelle marque ? », lui demandent les policiers en garde à vue. « Je sais pas, j'ai tout oublié. »
Une autre fois, il évoque une « 650, une BMW ». « Ça existe ? » « Faut que je réfléchisse », élude M, qui finit par avouer qu'il y avait bien 650 000 € à collecter.

Des agents américains infiltrés

C'est un accord d'entraide qui remonte à l'époque de la French Connection. Depuis 1971, les agents américains de la DEA (service de police fédéral qui lutte contre le trafic de stupéfiants) peuvent opérer en France. Ils l'ont fait à deux reprises dans le cadre du dossier Cedar. Une première fois, le 15 mai 2015, deux infiltrés se font passer pour des « cols blancs » voulant faire transiter des espèces. L'argent sera versé à Paris, puis déplacé à l'étranger par « compensation ». En planque, les policiers français ne perdent pas une miette de la scène, qui se joue dans un palace parisien. Les deux agents, un homme et une femme, montent dans la chambre de leur contact libanais. En quelques minutes, l'affaire est conclue. Le 28 août, rendez-vous est pris pour le versement, sur une célèbre terrasse des Champs-Elysées. Il est 23 h 20. M. le coursier du réseau, est à l'approche, au volant d'un discret Renault Scénic. L'homme est nerveux. Il appelle son patron, se plaint de ne voir personne, et s'inquiète que l'endroit grouille de policiers. « Il est niqué ce type ! Il m'a fait changer trois fois d'adresse », se plaint-il en évoquant l'agent de la DEA sous couverture. Finalement, les deux se retrouvent le long de l'avenue. En quelques secondes, à travers la vitre passager, M. récupère l'enveloppe. L'ensemble de la scène est immortalisé en photo. Domicilié aux Pays-Bas, le passeur a depuis fait l'objet d'une procédure judiciaire dans son pays de résidence.

Range Rover et Audemars Piguet

Quand l'argent est arrivé à destination, il faut alors le blanchir. Cette fois, les véhicules sont bien réels. Plusieurs intermédiaires sont alors sollicités. O.F. s'est fait une spécialité d'acheter en liquide des voitures en région parisienne. Le plus souvent à des garagistes peu regardants sur l'origine des fonds. Chaque année, il expédie au Liban une soixantaine de voitures de luxe, via la Belgique ou le port de Gennevilliers. Son engin de prédilection : le Range Rover, finition Autobiography. Un modèle à 140 000 €. « Je t'envoie le nouveau ! » dit-il à un de ses interlocuteurs. « Je veux le Mercedes. Le Range, au Liban, n'importe qui en a un ! » « Celui-là a une couleur qui n'existe pas là-bas. Magnifique. »
Deux de ces véhicules notamment sont achetés en espèces à un émir installé dans les Yvelines, réglés 158 000 € cash. O. reconnaît a minima qu'il avait eu des soupçons sur l'origine des fonds. « Je pensais que c'était de l'évasion fiscale, se défend-il. Je me sentais obligé. M. a rendu mes affaires plus florissantes. » Comme il a fait fleurir celles d'A.Z., marchand de montres reconnu, toujours en recherche d'espèces. Cela tombe bien, H. en a à revendre. Chaque année, A.Z. acquiert 120 montres en Allemagne, « un pays où les fournisseurs ne se soucient pas du cash ». Avec H. il va en recevoir du « sale », pour le rendre « propre » au Liban, une fois que les montres y ont été revendues. Rolex, Patek Philippe ou IWC, « elles valent en moyenne de 30 000 à 50 000 », calcule A. Voire 175 000 pour ce modèle Audemars Piguet exceptionnellement écoulé à Paris. Au total, A. dit avoir « 180 montres en stock », et freiner les reventes pour ne pas casser le marché libanais. Aucun problème de transport : les boîtes voyagent par colis, les montres avec des passeurs, avec la complicité du directeur de l'aéroport de Beyrouth. En sept remises, 1,3 million a été blanchi par A. en seulement quatre mois.
Pas assez selon lui, son business étant de plus en plus gourmand en espèces. « Il en a profité, mais ne pouvait plus faire machine arrière », tempère son avocat, M^e^ I. Ali

finit par remplacer H. à la collecte, récoltant 4 millions en six mois. Car H. a une détestable manie : prélever pour son compte une part de l'argent qu'il fait transiter. Un petit manège que ses donneurs d'ordre ont fini par découvrir. « Il doit 50 000 à l'un, 65 000 à un autre ! » s'énerve M.E., qui dit lui avoir expliqué « qu'il fallait qu'il règle le problème, ou je l'enterrais au centre de Beyrouth ».
Il n'aura pas le temps de mettre sa menace à exécution. H. est interpellé début janvier. La semaine dernière, il a été extradé par la France pour y être entendu par la justice.
Liens : http://www.leparisien.fr/faits-divers/l-argent-sale-transforme-en-montres-et-voitures-de-luxe-24-04-2016-5741047.php

La fin des cartes SIM anonymes, prisées des malfrats et des terroristes, est imminente…mais elle pourrait être inutile

Il faudra attendre l'automne pour que les opérateurs soient contraints de lier chaque carte SIM du pays à une identité. Cela fait pourtant près de 20 ans que les services de police dénoncent la dangerosité des cartes prépayées, qui peuvent être complètement anonymes en Belgique.
Depuis longtemps, on sait que les cartes prépayées font le bonheur des personnes malintentionnées, qui peuvent garder l'anonymat tout en commettant leur méfait, quel qu'il soit.
Il suffit en effet de se rendre dans n'importe quel commerce, et de payer en liquide une carte SIM avec un numéro de téléphone attribué, et une recharge d'un certain nombre de minutes/SMS/internet mobile.
On insère ensuite la carte dans un téléphone ou un smartphone, et on peut communiquer sans laisser la moindre trace. Mais cela est sur le point de changer, du moins en Belgique (ce qui va bientôt poser problème, nous le verrons).
"Un petit pourcentage reste anonyme"
Le premier opérateur du pays, Proximus, nous a confirmé que l'anonymat complet était une réalité, mais pas la règle. "*Les opérateurs cherchant toujours à mieux connaître les utilisateurs, ils favorisent ceux qui se font connaître*", nous a expliqué Haroun Fenaux, porte-parole.
L'intérêt de s'identifier sur le site de Proximus est de cumuler des points, de participer à des concours, d'avoir des bonus de recharge lorsque c'est fait en ligne.
"*Mais il reste effectivement un pourcentage de clients totalement anonymes, et c'est ceux-là que l'Etat désire connaître*".
Un grave évènement
Il aura fallu, comme c'est souvent le cas, un évènement très grave pour que la législation change. Les récents attentats de Bruxelles, en mars 2016, ont déclenché une prise de conscience collective de la nécessité d'enfin pouvoir lier une identité à un numéro de téléphone.
Car sans surprise, pour se coordonner et pour communiquer avant et pendant les attentats, les terroristes changent souvent de carte prépayée (anonyme), et donc de numéro de téléphone.
Rendant leur mise sur écoute très difficile, voire impossible, par les services de renseignements.
La fin de l'anonymat enfin annoncée mais…
Le 13 mai dernier, le gouvernement a enfin passé la seconde, annonçant la "*fin de l'anonymat des cartes SIM prépayées*". Les choses ont vite bougé ces dernières

semaines, mais le processus pour inscrire ce genre de règles dans la législation des opérateurs télécoms est long.
En réalité, il a débuté… avant les attentats de Bruxelles. Une consultation publique a été organisée du 7 au 14 décembre 2015 sur un avant-projet de loi modifiant l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques.
A cette époque, les cartes prépayées avaient été exclues du processus d'identification des utilisateurs, "*pour favoriser la pénétration de la téléphonie mobile*" (pour des raisons économiques, donc).

… les premières demandes datent de 1999

Autre constat étonnant: "*la suppression de l'anonymat pour les cartes prépayées est une revendication déjà ancienne des autorités judiciaires (1999)"*, car elles sont "*très répandues dans les milieux criminelles"*, peut-on lire dans cet avant-projet de loi.
Cela fait donc très, très longtemps qu'on connait le danger potentiel de ces cartes. Il est regrettable qu'il ait fallu attendre les drames de Paris et de Bruxelles pour concrétiser la fin de leur anonymat…
Quoi qu'il en soit, les choses s'accélèrent. "*Le projet de loi et le projet d'arrêté royal (...) vont à présent être soumis à l'avis du Conseil d'État et de la Commission pour la Protection de la Vie privée, avant d'être inscrit à l'ordre du jour du Comité de concertation. La nouvelle réglementation devrait entrer en vigueur cet automne après avoir été avalisée par le Parlement*", peut-on lire dans un communiqué du cabinet d'Alexandre De Croo, ministre fédéral des télécoms.
"*Une fois que les détails seront connus, on aura 6 mois pour se mettre en conformité*", nous a précisé de son côté Proximus. Il faudra donc attendre 2017 avant que les cartes SIM prépayées en activité en Belgique soient liées à une identité.

Concrètement, comment va-t-on identifier les cartes prépayées ?

La procédure est simple dans l'idée. La nouvelle réglementation obligera les opérateurs à appliquer le même principe d'identification des cartes SIM liées à un abonnement, à celles prépayées et qui peuvent être rechargées de manière anonyme.
Lorsqu'une carte prépayée sera achetée dans un magasin, la carte d'identité sera scannée et les données seront transmises à l'opérateur, ou si nécessaire, le commerçant fera une copie de la carte et les données seront également communiquées à l'opérateur.
En cas d'achat en ligne, l'identification se fera via la carte d'identité électronique (il faudra dès lors disposer d'un lecteur de carte), la signature électronique (liée à une carte d'identité), un service de contact certifié ou une transaction de paiement électronique.
Enfin, tous ceux qui utilisent déjà des cartes prépayées auront 6 mois pour s'identifier, de la même manière que ceux qui achètent une nouvelle carte prépayée.
Quant aux modalités de conservation des données de connexions, elles sont similaires à celles prévues depuis 2005 pour l'ensemble des "communications électroniques". La plus importante de ces modalités, c'est que les opérateurs doivent conserver ces données durant un an.

Orange prend les devants, des procédures compliquées en vue

Une procédure simple dans l'idée, on l'a dit, mais complexe dans la mise en œuvre. Comment être certain qu'un petit night-shop bruxellois soit en mesure de scanner une carte d'identité et de l'envoyer correctement à l'opérateur ? Le contrôle d'identité est encadré par la loi, n'importe qui ne peut pas se permettre de vérifier si la carte d'identité fournie est la bonne…
Dans ce contexte délicat, Orange (le nouveau nom de Mobistar), a décidé de prendre les devants. "*A partir de fin juin, une identification sera nécessaire pour acheter une*

carte SIM prépayée dans les magasins Orange faisant partie du réseau de distribution", nous a confirmé Jean-Pascal Bouillon, porte-parole.

Il s'agira plutôt d'un laboratoire pour expérimenter les procédures. Car comme le rappelle Orange, "*il y a de très nombreux points de vente (night-shop, magasins, etc) où l'on peut se procurer des cartes prépayées, et on ne peut pas les obliger à exiger l'identification des clients*".

Dans tous ces points de vente, donc, la mise en place d'un contrôle d'identité sera pour le moins délicate. Selon certains observateurs, c'est toute l'organisation de la distribution qui est à revoir.

Et si les nouvelles cartes SIM prépayées (pas les recharges) devenaient exclusivement disponibles dans les boutiques officielles des opérateurs, ou pourquoi pas dans les bureaux de *bpost*, les administrations communales, etc ? Cela représenterait un manque à gagner pour les opérateurs, mais cela simplifiera la procédure.

Du côté de Proximus, on confirme qu'il "*faudra analyser les procédures et le système de distribution*", et que cela se fera "*lorsque les opérateurs auront reçu tous les détails*" des autorités. Tout cela *"ne se fera pas du jour au lendemain"*.

Cela concerne combien de personnes ?

Fin 2013, les cartes prépayées représentaient **40%** des cartes SIM en circulation en Belgique, selon des chiffres de la GSMA, l'association mondiale des opérateurs mobiles.

Des chiffres qui ont changé dernièrement, suite à la chute des tarifs des abonnements. C'est ce qu'on peut comprendre des statistiques que Base a bien voulu nous fournir. Chez Base, les cartes prépayées représentent au moins un tiers des numéros Base, auquel il faut rajouter celles des opérateurs virtuels qui "louent" le réseau de Base.

"*Au total, le réseau Base héberge aujourd'hui un peu plus de 3 millions de clients. Parmi ces 3 millions de clients, 1 million sont des abonnés (clients* postpaid*), 1 million sont des utilisateurs de cartes prépayées (*prepaid*), et 1 million sont des clients de nos partenaires et des opérateurs virtuels que nous hébergeons (Mobile Vikings, Jim Mobile, Allo RTL, Ortel,...)*", nous a précisé François Bailly, porte-parole de Base Company.

Du côté d'Orange, les cartes *postpaid* sont encore moins nombreuses. "*Nous avons 3 millions de clients mobiles, dont 800.000 cartes prépayées, soit moins d'un tiers*", selon Jean-Pascal Bouillon.

80 pays obligent l'identification à l'achat d'une carte prépayée, mais c'est bientôt inutile…

Selon ce même rapport de la GSMA, en 2013, 80 pays obligeaient leurs citoyens à s'identifier à l'achat d'une carte prepayée ou envisageaient de le faire. La France, les Pays-Bas et l'Allemagne obligent par exemple les consommateurs à livrer leur identité lors de l'achat d'une carte prepayée. Ce qui n'a pas empêché les attentats de se commettre…

Enfin, sachez qu'au Luxembourg, le Premier ministre Xavier Bettel a annoncé, en 2015, le retrait de la vente des cartes prépayées.

Hélas, toutes ces initiatives nationales seront inutiles dans un an. En effet, en juin 2017, les opérateurs des pays de l'Union européenne ne pourront plus faire payer de frais de *roaming*. Téléphoner en Belgique avec une carte SIM prépayée italienne ne coutera donc pas plus cher que de téléphoner en Italie…

Vous l'avez compris, il faut donc impérativement une législation européenne pour que la fin de l'anonymat soit effective.

Nous avons sollicité le cabinet d'Alexander De Croo pour une réaction à ce sujet à plusieurs reprises, mais nous n'avons jamais obtenu de réponse.

Les cartes de crédit prépayées, même combat…
Un anonymat qui est également financier pour les terroristes: Salah Abdeslam a utilisé pendant plusieurs mois avant son arrestation une carte de crédit prépayée anonyme de *bpost* pour se déplacer dans toute l'Europe.
C'est Philippe de Koster, le directeur de la Cellule de Traitement des Informations Financières (CTIF) du blanchiment d'argent, qui l'a déclaré devant la Chambre, le 13 mai dernier. Il estime que ces cartes *"permettent le financement du terrorisme"*, et sont au moins aussi dangereuses que les cartes SIM prépayées.
"*Ces cartes sont l'instrument préféré des terroristes*", dit-il, déplorant la politique commerciale de *bpost*, qui cherche à promouvoir ces cartes anonymes alors qu'elles représentent à ses yeux un danger. 09 juin 2016
Liens : http://www.rtl.be/info/vous/temoignages/la-fin-des-cartes-sim-anonymes-prisees-des-malfrats-et-des-terroristes-est-imminente-mais-elle-pourrait-etre-inutile-821173.aspx

Les Ports Francs aimeraient serrer la vis

Antiquités et marché de l'artLe président de l'institution genevoise, David Hiler, regrette le manque de pouvoir de contrôle
D’abord parer au plus pressé – l’affaire des antiquités dites «du sang», qui relève autant du recel que du blanchiment, voire du financement du terrorisme. La direction des Ports Francs et Entrepôts de Genève a annoncé mardi la mise en place, dès cet été, d’un contrôle systématique des pièces archéologiques avant leur arrivé dans ses bâtiments.
Pour faire accepter un vestige, un dossier devra être rempli puis envoyé à une société de surveillance privée. «Si des doutes sont émis, un contrôle visuel de la marchandise sera exigé; si les incertitudes subsistent, l’avis d’un expert indépendant sera demandé», a détaillé Alain Decrausaz, directeur général de cette institution contrôlée à 87% par le Canton de Genève. Ce filtrage accru a été annoncé à l’occasion de la présentation de l’avancée de la mise en place de mesures destinées à «réduire les risques liés à l’exploitation d’un port franc».
Financement de Daech
La mobilisation est à la hauteur des pressions. En novembre, le directeur du Musée du Louvre soulignait combien les trafiquants d’antiquités – notamment celles en provenance de Syrie, soupçonnées de fournir une part importante de revenus à Daech – étaient capables de leur «inventer une histoire» en les stockant quelques années à Genève, au Luxembourg ou à Singapour. Des pièces archéologiques suspectes dont la présence vient ainsi à décrédibiliser le discours helvétique en matière de lutte contre le financement du terrorisme.
Paradoxe, ces contrôles accrus ne «vont pas empêcher d’autres affaires d’éclater», a prévenu hier le président des Ports Francs, David Hiler. Les pièces accueillies avec largesse en Suisse au cours des années 80 et 90 vont en effet continuer de remonter à la surface au fil de l’inventaire réalisé par les douaniers dans ces entrepôts. Plusieurs procédures sont en cours – elles s’étalent sur des années – dont une concernant un sarcophage romain identifié en 2010 et dont la restitution est exigée par la Turquie depuis.
Transparence partielle
Rien de nouveau en revanche n’a été annoncé hier en réponse à la principale critique adressée aux Ports Francs: leur absence de contrôle de l’identité des bénéficiaires

réels des objets qui y sont entreposés – souvent masqués par des sociétés-écrans, ou sociétés offshore.

L'institution va certes exiger à partir de la fin de l'année que les 223 locataires des espaces d'entreposages situés en son sein – grands transitaires comme Natural Le Coultre, marchands d'arts, galeristes – déclarent leur identité finale. Mais ni les douanes ni les Ports Francs ne sont tenus d'exiger l'identité du véritable bénéficiaire d'une toile de maître affublée d'une société-écran en guise de propriétaire.

Le Luxembourg a lui déjà adopté une solution plus stricte pour ses ports francs, qui avaient été créés par l'homme d'affaires genevois Yves Bouvier. Le Grand-Duché a dû réviser sa législation pour soumettre les transitaires aux mêmes obligations de contrôles antiblanchiment que ses banques. Ce qui leur impose d'exiger la divulgation de l'ayant droit final des pièces déposées. A l'inverse, le Conseil fédéral a, lui, décidé en novembre dernier de ne pas bouger sur ce point. (24 heures). 09.06.2016.

Liens : http://www.24heures.ch/suisse/ports-francs-aimeraient-serrer-vis/story/26757817