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 nombre de dossiers liés au financement du terrorisme en augmentation

Le nombre de nouveaux dossiers transmis aux parquets en rapport avec le terrorisme et le financement du terrorisme est passé de 35 en 2014 à 75 en 2015, révèle le rapport d'activités 2015 de la Cellule de traitement des informations financières (CTIF) publié vendredi.

Si l'on y ajoute les transmissions complémentaires relatives à des dossiers plus anciens, la part du terrorisme et du financement du terrorisme dans les transmissions 2015 est de 11% contre seulement 3% en 2014 et 2013. "Les premiers chiffres de 2016, influencés par les attentats de Bruxelles, confirment malheureusement la tendance", indique le rapport.

Sur cette question, la CTIF distingue le financement d'une organisation terroriste d'envergure comme l'Etat islamique, où les montants sont colossaux, et le financement d'attentats, dont ceux de Paris et de Bruxelles, où l'on parle plutôt de "micro-financement." Dans plus de 75% des cas, l'attaque planifiée par une cellule djihadiste coûtait moins de 10.000 dollars, selon la CTIF.

Les individus radicalisés et les combattants étrangers utilisent dès lors de plus en fréquemment des sources de financement à l'origine licite, telles que les allocations sociales ou les crédits à la consommation, pour financer leur voyage vers la Syrie ou la préparation d'attentats. Seule environ une cellule djihadiste européenne sur quatre reçoit de l'argent d'une organisation terroriste internationale, constate la CTIF.

La Cellule enquête sur base d'informations transmises par le secteur financier, essentiellement les établissements de crédit, l'administration ou encore les notaires. Elle transmet un dossier aux autorités judiciaires si elle estime que les charges sont suffisantes pour engager des poursuites.

Liens : http://www.7sur7.be/7s7/fr/32684/Menaces-terroristes-en-Belgique/article/detail/2796688/2016/07/15/Le-nombre-de-dossiers-lies-au-financement-du-terrorisme-en-augmentation.dhtml

Rapport d'activités 2015 de la CTIF

Plus de 3.600 dossiers transmis aux parquets, représentant plus d'un milliard d'euros

Si le nombre de déclarations de soupçon reçues par la Cellule de traitement des informations financières (CTIF) est resté relativement stable par rapport à 2014 (+1,82%), le nombre de nouveaux dossiers ouverts en 2015 a lui augmenté de manière considérable, à 8.329 en 2015 contre 6.978 en 2014, révèle le rapport d'activités 2015

du CTIF publié vendredi. Après analyse, 3.646 transmissions judiciaires aux parquets locaux et au parquet fédéral ont été effectuées, représentant un montant de 1,064 milliards d'euros. La Cellule de traitement des informations financières (CTIF) a noté l'an dernier une très légère augmentation (+1,82%) du nombre de déclarations de soupçons de blanchiment d'argent, de fraude grave ou de financement de terrorisme, par rapport à 2014. Ces déclarations de soupçon proviennent essentiellement du secteur financier (75%). Sur un total de 28.272 déclarations de soupçon, 13.376 concernaient de nouvelles affaires de blanchiment ou de financement du terrorisme et 14.896 étaient des compléments à des dossiers déjà existants.
Sur base de ces déclarations, l'analyse de la CTIF a donné lieu à 3.646 transmissions judiciaires aux parquets locaux et au parquet fédéral, soit 992 nouvelles transmissions et 2.654 transmissions complémentaires concernant des dossiers plus anciens. Le montant total des opérations présumées de blanchiment et de financement du terrorisme dans ces transmissions s'élève à 1,064 milliard d'euros.
En nombre de transmissions, l'escroquerie (21%) reste la principale criminalité sous-jacente présumée aux opérations de blanchiment communiquées aux autorités judiciaires, suivie essentiellement par la criminalité organisée (11%) et le terrorisme et financement du terrorisme (11%). Par contre, les montants de blanchiment répertoriés les plus importants concernent la fraude fiscale grave (322 millions d'euros), la criminalité organisée (225 millions) et le trafic de main d'oeuvre clandestine (133 millions). 15/07/2016
Liens : http://fr.metrotime.be/2016/07/15/news/rapport-dactivites-2015-de-la-ctif-plus-de-3-600-dossiers-transmis-aux-parquets-representant-plus-dun-milliard-deuros/

Des attentats financés par les salaires, les crédits et les allocations sociales

Combien coûte la préparation d'un attentat ? Dans 75 % des attentats commis en Europe entre 1993 et 2013, c'était moins de 10.000 dollars (9.000 euros), a calculé un institut de recherche norvégien en matière de défense. Soit moins qu'une voiture neuve…
La modicité de ces montants rend donc difficile la détection de telles cellules terroristes via le volet financier, relève dans son dernier rapport annuel la Cellule de traitement des informations financières (CTIF).
Chargée de la lutte contre le blanchiment, la cellule est également chargée de détecter les sources de financement du terrorisme. Son rôle a été renforcé dans ce domaine : les contacts avec le parquet fédéral et l'Ocam ont ainsi été fluidifiés depuis les attentats de Paris.
La CTIF a reçu l'année dernière 75 nouveaux dossiers, qui représentent autant de déclarations de soupçons. C'est deux fois plus qu'en 2014. *"Les premiers chiffres de 2016, influencés par les attentats de Bruxelles, confirment malheureusement cette tendance"*, relève Philippe de Koster, président de la CTIF.
La CTIF distingue le financement d'une organisation terroriste d'envergure comme l'État islamique, pour lequel les montants sont colossaux et le financement d'individus radicalisés en Syrie ou en Irak qui reviennent en Europe pour des attentats. Ici, les montants peuvent apparaître comme dérisoires. 18 juillet 2016
Liens : http://www.lalibre.be/actu/belgique/des-attentats-finances-par-les-salaires-les-credits-et-les-allocations-sociales-578bb440357086b3e0d2f08b

Des attentats toujours différents pour semer la terreur

Frapper là où on ne les attend pas. L'extrême diversité des moyens utilisés pour répandre la terreur est l'une des stratégies des organisations terroristes.

Un véhicule lancé dans la foule… Ce n'est pas la première fois que des terroristes utilisent cette "arme": en mai 2013 à Londres, et en octobre 2014 à Montréal, des terroristes avaient lancé leurs voitures contre des militaires.

Mitraillages, ceintures explosives, camion fou...

C'est cependant l'extrême diversité des moyens de répandre la terreur qui retient l'attention. Pour s'en tenir à notre pays, les terroristes ont frappé en janvier 2015 en attaquant avec des armes à feu deux lieux symboliques, les locaux de Charlie Hebdo et un supermarché casher.

En juin, un terroriste tue et décapite son patron à Chassieu (Rhône). En août, un homme tente de mitrailler les passagers d'un Thalys. En novembre 2015, c'est le massacre du Bataclan, et le mitraillage de plusieurs terrasses d'un quartier de Paris…

Débrouillez-vous pour tuer des des infidèles

Peu importe le moyen. "Si vous ne pouvez pas faire sauter une bombe ou tirer une balle, débrouillez-vous pour vous retrouver seul avec un infidèle français ou américain et fracassez-lui le crâne avec une pierre, tuez-le à coups de couteau, renversez-le avec votre voiture...", lançait récemment un responsable syrien de Daech.

Pas besoin de beaucoup d'argent

Pas besoin de beaucoup d'argent pour agir ainsi. Il existe certes des filières de financement du terrorisme, du pétrole aux œuvres d'art. Mais louer un camion est à la portée de chacun. Et le coût des massacres du 13 Novembre a pu être évalué, dans une comptabilité macabre et dérisoire, à 30 000 euros.

Choquer les touristes du monde entier

Dans tous les cas, l'objectif est de faire peur au plus grand nombre. C'est même la définition du terrorisme retenue par les Nations Unies: "Les actes criminels qui, à des fins politiques, sont conçus ou calculés pour provoquer la terreur dans le public".

Et comment mieux frapper les imaginations, qu'en attaquant des cibles symboliques : un journal satirique pour attaquer la liberté de la presse, un supermarché casher pour agresser tous les Juifs, la Promenade des Anglais à Nice, qui plus est un 14 Juillet, pour choquer les touristes du monde entier…

Plus le symbole est fort, plus le retentissement est important, dans une logique spectaculaire entretenue par la surenchère médiatique de notre époque.

Au mauvais endroit, au mauvais moment

Mai une autre dimension se développe avec cet attentat de Nice : la conscience que tout le monde peut être victime d'un acte terroriste, qu'il suffit pour cela d'être au mauvais endroit au mauvais moment. C'était le cas des milliers de personnes qui assistaient au feu d'artifice de Nice.

Comme des centaines de jeunes Parisiens prenant un verre en terrasse, le soir du 13 novembre. Ou encore des passagers du Thalys Amsterdam-Paris, qui n'ont dû qu'à l'héroïsme d'un soldat américain d'échapper à un massacre.

"Je ne savais plus quoi faire"

La boucle est alors bouclée, le climat de terreur est entretenu d'un acte à l'autre. "J'étais au Stade de France le 13 Novembre. Et quand j'ai reçu hier soir l'alerte sur

l'attentat de Nice sur mon portable, j'assistais au feu d'artifice à Paris, sur les bords de Seine… Je ne savais plus quoi faire, si je devais partir ou non", témoigne Gautier. C'est cela, la logique de la terreur à laquelle il faut apprendre à résister.
Liens : http://www.dna.fr/actualite/2016/07/15/des-attentats-toujours-differents-pour-semer-la-terreur

[Attentats] Le chiffrement, cette cible perpétuelle

À chaque nouvel attentat frappant l'Europe, les dirigeants dénoncent le chiffrement utilisé par les terroristes pour passer entre les mailles du filet. Oubliant opportunément de faire état d'enquêtes pointant l'utilisation de téléphones jetables par les terroristes.
« *Ceux qui nous frappent utilisent le Darknet et des messages chiffrés* ». Mercredi, lors des questions au gouvernement Bernard Cazeneuve était affirmatif. Sans nuance. Et pourtant, le ministre de l'Intérieur semble (opportunément ?) oublier le rapport émis par ses propres services sur les attentats du 13 novembre dernier, qui ont tragiquement frappé la capitale faisant 130 morts et plus de 400 blessés.
Un rapport que n'a pas manqué de relayer le *New York Times*. Long de 55 pages, ce rapport indique que les enquêteurs n'ont trouvé aucune trace d'utilisation de messagerie chiffrée ou d'utilisation d'outil de ce type par les terroristes. Pour organiser les attentats, il s'avère qu'ils ont privilégié l'utilisation de téléphones jetables (prépayés), comme celui retrouvé dans une poubelle non loin du Bataclan, avec pour tout SMS, non chiffré, « *on est parti on commence* ». Ce téléphone avait été activé seulement une heure avant le début de l'opération. Des téléphones encore inutilisés et emballés ont même été retrouvés chez les suspects.
Les trois commandos « *n'ont utilisé que des nouveaux téléphones dont ils se débarrassaient ensuite, dont certains activés seulement quelques minutes avant les attaques, ou des téléphones qu'ils prenaient sur leurs victimes* », rapporte ainsi le quotidien américain.
Cet article du *NYT* a d'ailleurs donné lieu à une passe d'armes entre Snowden et le créateur de la série *The Wire* David Simon sur Twitter autour de la surveillance, exposant deux approches différentes de la surveillance électronique.
L'une appliquée à la lutte contre le terrorisme, telle que la conçoit la NSA, massive et indiscriminée, l'autre pour combattre la criminalité.
Snowden rappelle d'ailleurs qu'en matière de terrorisme, « *dans les opérations de la vie réelle les téléphones sont utilisés pour une action, un appel. Leur durée de vie se compte en minutes, en heures. Pas en jours* ». Il serait alors vain de vouloir les isoler pour repérer les terroristes via des écoutes notamment.
Quand bien même un message apparu sur Telegram peu après les attentats de Bruxelles et attribué à l'organisation État islamique (OEI) conseillerait à ses « *frères* » d'éviter les réseaux sociaux et d'utiliser des outils de chiffrement, aucun élément n'est venu confirmer cet usage. Certains experts estiment même que ce message est trop « *simple* » pour être vrai.
L'utilisation de l'application sécurisée Telegram par l'organisation pour communiquer avec ses partisans ne vaut pas preuve de l'utilisation de ce même genre d'outil pour la préparation d'attentats. D'autant que ces services sont particulièrement surveillés par les autorités.
Mais pour ces dernières, le simple fait de n'avoir rien trouvé, vaut preuve, comme le relève encore le *NYT* : « *Selon le rapport de police et des interviews menées avec des*

responsables, aucun des emails des terroristes ni un autre type de communication électronique n'a été découvert, ce qui amène les autorités à conclure que le groupe a utilisé le chiffrement. On ne sait pas quel genre de chiffrement, et cela fait partie des détails que la capture de Salah Abdeslam permettrait de révéler. »

Ces quelques lignes ont suscité l'ire des défenseurs du chiffrement, comme le souligne justement Slate relayant un article de TechDirt :

« Mais… le chiffrement ne marche pas comme ça. S'ils utilisent des emails chiffrés, les emails ne disparaissent pas. On peut toujours voir qu'ils existent, et les métadonnées qui indiquent qui a envoyé le message à qui restent là. C'est juste qu'on ne peut pas lire les contenus des emails. […]

Bien sûr qu'il est possible que les terroristes aient utilisé un moyen secret pour communiquer, mais le problème, alors, n'est pas le chiffrement, mais plutôt qu'ils ont trouvé un moyen de cacher ce moyen par lequel ils ont communiqué. Ou alors, vous savez, ils sont allés se parler directement, face à face. »

L'organisation utilise probablement des outils de chiffrement, tout comme elle a très bien pu élaborer son propre outil, il serait donc absurde de vouloir interdire ou affaiblir le chiffrement dans son ensemble, notamment en donnant une *clé d'accès* aux autorités. Le secret serait rapidement éventé et les organisations terroristes trouveraient rapidement une alternative.

Le fondateur de Telegram, Pavel Durov, se confiait à Wired à ce propos en février dernier :

« À chaque fois que l'on aborde ces sujets, nous devons prendre en compte le fait que ceux d'en face vont réagir. Ils ne vont pas continuer à faire comme avant. Si l'on imagine qu'une application de messagerie populaire implémente des portes dérobées ou commence à partager des données avec les autorités, il sera impossible de garder ce secret très longtemps. […] Mais si cela se produit, alors ces méchants changeront de moyen de communication.

Les algorithmes de chiffrement de bout en bout ont déjà fait l'objet de beaucoup d'études et sont bien connus, et ils pourraient être utilisés par qui que ce soit, pour le bien ou le mal. Et si Telegram ou d'autres services deviennent vulnérables ou s'ils ne sont pas sécurisés, alors les terroristes n'auront aucun problème à utiliser une nouvelle application et probablement une qu'ils auraient créée eux-mêmes. »

Le chiffrement n'est pas seulement un outil utilisé par les délinquants et terroristes de tous bords, c'est également un moyen de protéger les citoyens et les gouvernements. Les États-Unis sont d'ailleurs une cible privilégiée de ces attaques et ont essuyé des cyberattaques dévastatrices (Sony Pictures, OPM, Pentagone, etc.).

Tim Cook, le CEO d'Apple n'a d'ailleurs cessé de le marteler : affaiblir le chiffrement et offrir un accès aux autorités via une porte dérobée, ouvrirait une « *boite de Pandore* » qu'il sera difficile de refermer.

S'exprimant sur la nouvelle loi de Renseignement britannique, qui entend interdire le chiffrement de bout-en-bout, le CEO d'Apple expliquait alors qu'« *une clé laissée sous le paillasson ne serait pas bon que pour ceux qui veulent faire le bien. Les méchants, la trouvera également* ». Soulignant qu'il est impossible de garantir l'accès aux *backdoors* aux seules personnes bien intentionnées.

Qu'en est-il du Darknet évoqué par Bernard Cazeneuve ? Le ministre assure qu'il est utilisé pour fournir des armes à l'organisation. S'il est effectivement possible de se procurer une arme sur différents marchés noirs en ligne, il serait bien étonnant que l'OEI s'en serve pour ses propres besoins. Premièrement parce que ces derniers ne se résument pas à l'achat d'une kalachnikov et que son envoi par La Poste à une adresse précise parait peu crédible.

Les reliquats des guerres d'ex-Yougoslavie et les armes provenant d'Europe de l'Est circulent beaucoup plus facilement et en nombre dans toute l'Europe.
Avec les bons contacts, dans les milieux concernés, il est relativement aisé de s'en procurer. La Belgique serait également devenue une plaque tournante du trafic d'armes. Les armes utilisées par les frères Kouachi et Amedy Coulibaly ont par exemple été achetées à Bruxelles, où il est relativement aisé d'acquérir une kalachnikov pour 1 000 à 2 000 euros.
Sur le même tempo que l'administration américaine, faisant "*siennes*" les préoccupations du gouvernement US, les déclarations de Bernard Cazeneuve contre le chiffrement semblent cacher un autre dessein. Comme dans l'affaire opposant le FBI et Apple, cette attaque servirait surtout les intérêts des forces de l'ordre qui verraient leur tâche grandement facilitée à l'avenir. Après la loi Renseignement et le projet de loi sur la réforme pénale, elles n'en demandaient peut-être pas tant. 24 mars 2016
Liens : http://www.journaldugeek.com/2016/03/24/attentats-chiffrement-cible/

[Attentats] Le chiffrement des communications (re)mis en cause

Plusieurs médias français et anglo-saxons pointent du doigt l'usage de messageries chiffrées par les terroristes du groupe État islamique, dont ceux des attentats de Paris. La CIA en profite pour tirer la sonnette d'alarme.
Depuis vendredi dernier, des voix s'élèvent pour dénoncer les messageries chiffrées ayant permis aux auteurs des attaques terroristes de Paris de communiquer librement entre eux sans craindre d'être interceptés par les autorités.
Si dans un premier temps certains médias ont évoqué l'usage de la PS4 pour planifier les attentats avant que l'information ne soit fortement remise en cause, d'autres ont immédiatement pointé du doigt les applications de messagerie chiffrée : Kik, Surespot, Wickr mais aussi Telegram. L'organisation État islamique utilisant cette application comme outil de propagande.
En effet, celle-ci offre plusieurs avantages : elle est gratuite, disponible sur la plupart des OS, et en version web, libre de modifications spécifiques adaptées à l'usage de son utilisateur, est très simple d'utilisation, permet d'envoyer des documents de toute taille, d'ouvrir des conversations de groupe allant jusqu'à 200 personnes, de programmer l'auto-destruction de certains messages et offre toutes les fonctionnalités d'une messagerie chiffrée.
De plus, l'application est soutenue par deux frères, dont le libertarien Pavel Durov. Son indépendance vis-à-vis de tout gouvernement – il s'est récemment exilé de Russie trouvant son climat peu propice aux affaires – l'a déjà vu tenir tête au Kremlin et à l'Iran.
Il n'en fallait pas plus pour que le chiffrement soit remis en cause et que les autorités s'engouffrent dans la brèche. Depuis plusieurs mois, FBI, CIA, GCHQ, NSA et même le procureur de Paris, François Molins, dans une tribune publiée dans le New York Times en août dernier, demandent que des choses soient faites contre la course au chiffrement opérée par plusieurs acteurs de des nouvelles technologies : Apple, Google et WhatsApp pour ne citer qu'eux, notamment depuis les révélations d'Edward Snowden sur le système de surveillance planétaire de l'agence de sécurité nationale américaine.
Pour le monde du renseignement US, un seul coupable est à blâmer : l'ancien analyste de la NSA, aujourd'hui réfugié en Russie où il bénéficie de l'asile politique.

Le directeur de la CIA, John Brennan, estime que l'agence n'a pas les moyens suffisants pour surveiller les terroristes :
« Ces dernières années, à cause de divulgations non autorisées et d'interminables demandes de mea culpa sur le rôle du gouvernement dans sa manière de traquer des terroristes, il y a eu des amendements aux lois et des actions qui ont été décidées qui ont rendu la tâche de débusquer les terroristes bien plus ardue pour nous. »
James Woolsey, ancien directeur de la CIA, va plus loin et estime quant à lui que Snowden a « *du sang sur les mains* ». Les dernières réformes entreprises par Obama auraient affaibli la communauté du renseignement et permis que les attentats de Paris se produisent. Opposons lui que la réforme entreprise par l'administration américaine est toute relative…
« *Je pense que nous allons apprendre que ces gars communiquaient via des applications chiffrées, ce chiffrement est très difficile, voire impossible à briser pour les gouvernements, et la loi ne permet plus aux éditeurs de fournir les clés nécessaires pour les déchiffrer* », a assuré Michael Morell, ancien directeur adjoint de la CIA dans une interview donnée à CBS.
Opportunisme ou réel besoin ?
Pour la presse américaine, Brennan se sert des attentats pour légitimer la surveillance de masse et servir les intérêts de l'agence. Même si Snowden a mis en lumière le système de surveillance de la NSA, il est peu probable que les terroristes aient attendu ces révélations pour agir et opter pour ce type de solutions offrant une discrétion à leurs communications. Pléthore de logiciels et app existent. Arstechnica souligne même que le chiffrement est utilisé depuis plus de 15 ans par les organisations terroristes.
Par ailleurs, les services de renseignement disposent d'une palette d'outil pour suivre et surveiller leurs cibles et toute technologie de chiffrement est potentiellement cassable. Les services du monde entier sont dotés d'outil de déchiffrement. Rien qu'en France, avec le controversé « PNCD » (Pôle national de cryptanalyse et de décryptement) tout juste légalisé par la loi Renseignement.
Accuser ainsi le chiffrement semble donc un moyen de relancer le débat des *backdoors* légales souhaitées par nombres de gouvernements. Le Royaume-Uni encore récemment avec sa loi renseignement offrant de larges prérogatives à ses agences gouvernementales.
Ce type d'événement voit régulièrement un renforcement des lois sécuritaires. Les dernières déclarations du président de la république devant le congrès en donne un aperçu. Le peuple est souvent peu enclin à protester saisi d'effroi. Au lendemain des attentats, un sondage Ifop pour RTL et *Le Figaro* révélait que 84% des personnes interrogées sont prêtes à accepter davantage de contrôles et une certaine limitation de leurs libertés pour mieux garantir la sécurité.
En France, Axelle Lemaire, secrétaire d'État au Numérique, assurait que le gouvernement misait sur le « *chiffrement systématique et par défaut des données entre les services de messagerie* ».
Mais ça, c'était avant.
Liens : http://www.journaldugeek.com/2015/11/18/attentats-chiffrement-communications-remis-en-cause/

[AppleVsFBI] Après Barack Obama, Cazeneuve prend position sur le chiffrement

Présent au festival SXSW ce week-end à Austin, le président américain Barack Obama s'est exprimé sur la bataille que se livre Apple et le FBI autour du chiffrement. Il demande à la Silicon Valley de faire des « ***concessions*** » avant que le législateur ne s'en mêle. Le ministre de l'Intérieur Bernard Cazeneuve dit faire« siennes » les préoccupations de l'administration américaine.

Premier président de l'histoire à répondre présent à l'invitation du Festival South by Southwest (SXSW), Barack Obama s'est exprimé sur la bataille opposant Apple et le FBI. Sans véritablement prendre parti, il a vivement incité les entreprises high-tech à trouver une solution qui satisferait les deux parties.

Utilisant la métaphore de la maison, Obama a expliqué que depuis 200 ou 300 ans, les Américains se laissaient déposséder d'un peu de leur vie privée pour garantir leur propre sécurité. Ainsi, les forces de l'ordre peuvent pénétrer dans la maison d'un suspect pour effectuer une perquisition à la recherche de preuves ou fouiller ses habitants, mais avec le chiffrement cela reviendrait à se trouver devant une maison sans serrure, ni porte.

« *Comment résoudre ou arrêter une attaque terroriste ?* », demande-t-il alors. Pour lui, un « *chiffrement solide* […] *fétichise nos téléphones en les plaçant au-dessus de toute autre valeur* » et va « *à l'encontre de l'équilibre que notre pays a atteint depuis deux cents ou trois cents ans* ».

Bien évidemment, en accord avec ses précédentes déclarations, il plaide pour un chiffrement et une clé « *les plus solides possible* ». Toutefois il rêve d'un monde qui allierait un chiffrement fort et possibilité laissée aux autorités d'accéder aux données souhaitées, mais « *dans un certain nombre de cas sur lesquels nous devons nous mettre d'accord* ».

Le président craint qu'en l'absence de consensus, le législateur ne s'empare du sujet et n'édicte une loi « *dangereuse* ».

Relativement absent du débat, le ministre de l'Intérieur a finalement pris parti… pour le FBI. Pour rappel celui-ci souhaite accéder aux données chiffrées de l'un des suspects de la tuerie de San Bernardino stockées dans son iPhone 5C.

Cette prise de position du ministre n'a rien de surprenant quand on se rappelle ses déclarations après les attentats de Paris de janvier 2015 et sa rencontre avec les géants du web, en marge du premier sommet international de lutte contre le terrorisme à Washington, qu'il entendait rallier à sa cause.

« *Je comprends parfaitement la préoccupation de l'administration américaine et je la fais mienne* », a-t-il assuré lors d'une intervention à l'université George Washington relative à la lutte antiterroriste.

« Je ne pense pas qu'il faille engager un bras de fer » avec ces entreprises proposant le chiffrement des communications à leurs utilisateurs, car elles auraient « intérêt à être nos partenaires. »

« *L'écosystème du numérique, c'est la démocratie. Si la démocratie n'est pas capable de se défendre elle-même, l'écosystème s'effondre. Il faut impérativement trouver des procédures et sous le contrôle et l'autorité du juge* ». Juge relativement absent des dernières lois adopté en matière de lutte contre le terrorisme…

Récemment, le journal britannique *The Guardian* révélait que les principaux géants du web se dirigeaient vers un renforcement du chiffrement proposés sur leurs services en optant pour le chiffrement de bout-en-bout (end-to-end). C'est à dire que seuls les

utilisateurs détiendront la clé de chiffrement à même de déverrouiller leurs données. Même sur demande des autorités munies d'un mandat, il sera alors impossible pour ces firmes d'accéder à leurs requêtes. On est encore loin du consensus…6 mars 2016
Liens : http://www.journaldugeek.com/2016/03/16/apple-fbi-obama-cazeneuve-chiffrement/

[Chiffrement] Après Apple, Whatsapp dans la ligne de mire ?

L'application de messagerie sécurisée Whatsapp serait la prochaine cible des autorités dans la guerre qu'elle mène contre la course au chiffrement des géants du web, révèle le ***New York Times***.
Il n'est pas question d'iPhone, d'Apple ou de terrorisme ici, néanmoins le problème reste le même : le chiffrement.
Dans le cadre d'une enquête en cours, un juge fédéral américain a donné son feu vert aux autorités pour procéder aux écoutes des communications passées depuis l'application de messagerie sécurisée Whatsapp. Problème, avec le chiffrement de bout en bout des communications proposées par la société depuis 2014 cela se révèle compliqué et l'enquête stagne.
Le Département de la Justice (DOJ) étudierait donc actuellement des solutions de contournement et des pourparlers seraient engagés entre Whatsapp et le DOJ, rapporte le *New York Times*.
Toutefois, alors que le contexte est déjà tendu et voit Apple et le FBI se livrer une guerre de tranchées autour de la sécurité des données et des communications, des sources proches du dossier assurent que le problème est autrement plus préoccupant dans cette affaire.
Pour le *NYT*, cela ouvrirait « *un nouveau front dans la contestation entre l'administration Obama et la Silicon Valley autour du chiffrement, de la sécurité et de la vie privée* ». Avec le chiffrement, l'avenir des écoutes électroniques serait en jeu. Écoutes que les agences de renseignement estiment être à la base de toute enquête criminelle.
La question étant désormais de savoir si le Département de la Justice doit forcer Whatsapp à aider le gouvernement afin qu'il obtienne ces informations, au risque de voir s'aggraver le conflit. De leur côté, les sénateurs seraient sur le point de légiférer concernant les sanctions civiles à imposer aux entreprises high-tech, qui refuseraient de répondre aux ordonnances du tribunal requérant leur coopération pour aider les autorités à accéder aux données chiffrées de leurs utilisateurs.
Un conflit juridique avec Whatsapp pourrait également inciter les législateurs à réviser la loi sur les écoutes (*wiretapping*) dont la dernière mise à jour remonte à une génération.
Pour l'Electronic Frontier Foundation (EFF), le FBI et le ministère de la Justice attendent juste le moment et le cas opportuns pour effectuer une demande qui apparaîtrait enfin raisonnable.
Whatsapp n'est pas la seule application chiffrée existante – Telegram serait d'ailleurs privilégiée par les djihadistes de l'organisation Etat islamique (OEI) pour communiquer – mais avec 1 milliard d'utilisateurs, elle est, de loin, la plus importante.
Le chiffrement n'est pas qu'une sécurité pour les clients des géants du web, c'est aussi un moyen pour le gouvernement de se protéger des cyberattaques dont il est

régulièrement victime. C'est pourquoi la Maison Blanche avait opéré un revirement sur le chiffrement en expliquant qu'il ne fallait en aucun cas l'affaiblir. Puis avait à nouveau changé d'avis peu après « *l'acte terroriste* » du 2 décembre perpétré à San Bernardino en Californie et revendiqué par l'organisation État islamique.
Au sein même de l'administration Obama, les avis divergent sur la manière d'inciter les entreprises high-tech à coopérer et/ou répondre aux requêtes des forces de l'ordre. La Maison Blanche a refusé de légiférer en ce sens en imposant des *backdoors* aux firmes technologiques et fait depuis des pieds et des mains pour s'attacher la coopération active des géants du web… qui semblent freiner des quatre fers, pris en étau entre la sécurité des données de leurs clients et les impératifs de sécurité nationale qui semblent légitime dans le contexte actuel. Google, Facebook, Snapchat et Whatsapp s'apprêteraient même à accélérer sur le chiffrement en optant pour le *end-to-end* sur l'ensemble de leurs services.
Un juste équilibre est-il possible ? Une solution qui allierait un chiffrement fort, et la possibilité laissée aux autorités d'accéder aux données souhaitées. Le président Obama la appelé de ses vœux et ce, avant que le législateur ne vienne imposer une loi qu'il juge « *dangereuse* ».
La vie privée est une notion très importante chez Jan Koum, le fondateur de Whatsapp, ce dernier ayant grandi sous l'ère soviétique en Ukraine. Il fut l'un des premiers à manifester son soutien à Tim Cook lorsque le CEO d'Apple a publié sa lettre ouverte expliquant les raisons de son opposition au FBI.
« *Notre autonomie et notre liberté sont en jeu* », avait-il alors déclaré sur sa page Facebook. 15 mars 2016
Liens : http://www.journaldugeek.com/2016/03/15/chiffrement-whatsapp-ligne-mire/

Sans chiffrement, pas d'attentats de Paris pour la NSA

Le directeur de la NSA assure que les autorités compétentes, dont l'agence de sécurité nationale américaine, n'ont pas pu détecter les terroristes et empêcher la tuerie qui s'en est suivie à cause des outils de chiffrement des communications utilisés pour leurs échanges.
C'est une déclaration qui tombe à point nommé, au moment même où Apple et le FBI s'affrontent sur la nécessité pour les autorités d'accéder aux données chiffrées des clients d'entreprises high-tech suspectés de terrorisme. Aujourd'hui, le directeur de la NSA, Michael Rogers vient apporter sa pierre à l'édifice.
Dans une interview donnée à Yahoo News, il met en cause le chiffrement dans la survenance des attentats du vendredi 13 novembre 2015. Il revient sur la prétendue utilisation d'outils de chiffrement des communications par les terroristes dans le cadre de la préparation des attentats de Paris.
Grâce à ces outils, ils ont pu passer entre les mailles du filet et ont réussi à déjouer la surveillance de la NSA et des différentes agences de renseignement : « *certaines communications* » des terroristes étaient « *chiffrées* ».
Nous n'avons pas généré de renseignement en amont, clairement si on avait su, Paris n'aurait pas eu lieu.
Ce qui peut paraître assez logique… à ceci près qu'il ne précise pas si la NSA était sur leur piste ou si elle a depuis récupéré des informations importantes. D'autant que l'enquête a révélé les failles béantes du renseignement belge et français, voire même européen.

Par ailleurs, l'étude des communications passées par les assaillants à partir d'appareils récupérés par les autorités démontre qu'ils échangeaient via des SMS standard et non des applications de messagerie chiffrées. À l'image du SMS qui avait donné le départ de l'attaque contre le Bataclan le 13 novembre au soir.
Rien ne dit non plus que sans chiffrement les attentats de Paris auraient pu être évités. Si les révélations d'Edward Snowden ont bien montré une chose, c'est que la surveillance de masse ne résout pas tout : elle ne permet pas de déjouer toutes les attaques fomentées. Trop d'informations rend aveugle quand on ne sait pas où chercher, ni comment analyser une masse conséquente de données.
Plus largement, Mike Rogers revient sur les informations selon lesquelles l'organisation État islamique (OEI) utiliserait des outils de chiffrement pour communiquer. L'OEI disposerait même d'un centre d'aide au chiffrement pour ses djihadistes.
Est-ce que nous avons du mal à acquérir les informations que l'on voudrait sur ces cibles ? Oui. Est-ce que c'est lié aux changements qu'ils font dans leur manière de communiquer ? Oui. Est-ce que le chiffrement rend nos missions plus difficiles à accomplir ? Oui.
Pour autant, il ne remet pas en cause le bien-fondé du chiffrement, comme il l'avait expliqué en début d'année.
« *Le chiffrement est fondamental pour le futur, et je ne pense pas que la question soit de savoir s'il faut s'en débarrasser.* […] J*e ne pense pas que ce soit réaliste*. »
Il souhaite simplement que ces entreprises puissent être en mesure de déchiffrer des données sécurisées si les autorités le requièrent. Ravivant ainsi le débat autour des *backdoors* dites légales. Ce à quoi s'oppose avec force Apple et d'autres entreprises de la Silicon Valley. Google et WhatsApp lui ont déjà apporté leur soutien.
La firme de Cupertino a toujours argué qu'il était impossible de créer une porte dérobée qui ne serait utilisable que par des personnes bien intentionnées, les autorités en l'occurrence, et qu'elle serait à la disposition de qui voudrait bien la trouver (gouvernements étrangers, mafia, hackers chevronnés).
De même, d'autres pays pourraient formuler des demandes similaires, la Chine, l'Iran ou la Russie. Que faudra-t-il leur répondre ?
Tim Cook, le CEO d'Apple, ne manque pas de souligner que cela affaiblirait la sécurité de ses produits, porterait atteinte à la vie privée de ses utilisateurs, mais aussi à son business. Apple a notamment dû montrer patte blanche pour avoir droit de cité en Chine.
Le vif débat entamé depuis mardi et l'injonction faite à Apple d'aider le FBI à déchiffrer l'iPhone 5C de l'un des auteurs de l'attentat de San Bernadino (Californie) ayant fait 14 morts le 2 décembre dernier, n'est qu'un épisode de plus dans cette bataille larvée entre la Silicon Valley et les agences gouvernementales.
Pour les autorités, le chiffrement complique énormément leur travail d'enquête, voire les rendent « *aveugle* » pour reprendre les termes du procureur de Paris François Molins dans sa tribune parue dans le *New York Times*.
Mais rien ne dit que l'absence de chiffrement aurait rendu la tâche des autorités gouvernementales plus aisée. 18 février 2016
Liens : http://www.journaldugeek.com/2016/02/18/chiffrement-attentats-paris-nsa/

Le Royaume-Uni renonce aux backdoors (ou presque)

Cette semaine la ministre de la Sécurité et de la protection en ligne, Joanna Shields, a assuré que le gouvernement britannique renonçait à réclamer des backdoors pour les services de renseignement et de sécurité tout en précisant qu'ils doivent être capables d'accéder à ces données sous présentation d'un mandat.

Elle a reconnu le « *rôle essentiel* » joué par un chiffrement fort dans la protection des données personnelles des internautes, faisant ainsi directement écho au renoncement de l'administration américaine.

« L'exécutif reconnaît le rôle essentiel que joue un chiffrement puissant dans la protection des données personnelles, des discussions et des échanges. Il ne préconise pas ni n'exige la fourniture d'une *backdoor*, pas plus qu'il ne soutient un tel affaiblissement arbitraire de la sécurité des applications et des services. De tels outils menacent l'intégrité même d'Internet », a-t-elle assuré.

Comme le rapporte Wired, la ministre s'exprimait devant la Chambre des Lords sur des questions relatives à la cybersécurité.

« *Ce n'est pas une question de création de backdoor, mais de possibilité pour les entreprises d'accéder aux communications sur leurs réseaux lorsqu'un mandat leur est présenté* », a expliqué Joanna Shields.

« *La législation actuelle exige des entreprises qu'elles fournissent un accès ciblé, sous réserve d'un mandat, aux communications de ceux qui cherchent à commettre un crime ou causer de graves dommages au Royaume-Uni ou à ses citoyens* ».

Renoncer aux *backdoors* mais demander des portes dérobées légales. Si le terme change, n'est-ce pas finalement la même chose ?

Pour Edward Snowden c'est du pareil au même puisque soumettre un mandat pour accéder à ces données chiffrées suppose l'existence d'une *backdoor* ou que les entreprises prennent leurs dispositions pour en trouver et déchiffrer ces données.

Ces déclarations, même si elles semblent encourageantes, restent en contradiction avec la volonté des géants du web d'accélérer et développer les moyens d'offrir un chiffrement des données personnelles à leurs clients. À l'image d'Apple sur iOS9 ou de WhatsApp (propriété de Facebook) qui propose un chiffrement de bout-en-bout des communications.

Autrement dit, l'utilisateur est le seul détenteur de la clé de chiffrement à même de déchiffrer ses données. Même avec un mandat établi en bonne et due forme et délivré par un juge, les autorités ne pourraient exiger d'Apple un accès aux data demandées puisque la firme sera dans l'incapacité de leur fournir. Seules les données stockées dans le *cloud* sont accessibles.

Une situation que Joanna Shields trouve « *alarmante* », rejoignant ainsi le premier ministre David Cameron, du moins dans ses dernières déclarations.
Ce dernier n'a jamais caché sa volonté de s'attaquer au chiffrement. Peu après les attentats perpétrés contre *Charlie Hebdo* et l'Hyper Casher de Vincennes, il dénonçait les applications de messagerie chiffrée (type WhatsApp, Skype, Hangout et iMessage), coupables d'octroyer un « *espace sûr* » aux terroristes, criminels et pédophiles.

« Dans notre pays, pouvons-nous autoriser un moyen de communication entre des personnes, même des extrémistes … que nous ne pouvons pas lire ? », s'interrogeait-il. « Non, il ne faut pas […] Le premier devoir de tout gouvernement est de garder notre pays et notre peuple en sécurité. » David Cameron

Soutenant ainsi le GCHQ, la FBI et la NSA.
Resurgit toujours cette nécessité d'offrir une réelle protection des données personnelles aux citoyens/internautes et celle de permettre aux autorités d'enquêter et résoudre des enquêtes criminelles. Apple justifie son chiffrement de bout-en-bout et le refus des *backdoors* par le fait qu'il ne peut être garanti qu'une porte dérobée ne soit utilisée que par des personnes *bienveillantes*. Mais de la même façon : les nouvelles technologies, à la portée de tous, et le chiffrement avec elles, sont également susceptibles d'être utilisées par des criminels au dessein funeste.
La solution parfaite existe-t-elle ? La BBC avance celle-ci : le gouvernement britannique pourrait obliger les citoyens à enregistrer leurs mots de passe dans une base de données accessible aux autorités uniquement sous mandat.
Aujourd'hui, il n'est plus véritablement question de chiffrement, de backdoors ou de mandat, mais semble-t-il de confiance. Qui n'existe plus ou est fortement ébranlée. Imaginons qu'une telle solution soit mise en place : quelle garantie que les autorités passent réellement par la case mandat, qu'elles ne cherchent pas, en cas de refus ou d'urgence, à contourner le problème et accéder aux données par leurs propres moyens ou que les entreprises hébergeant cette base de données, ces clés de chiffrement et autres mots de passe ne collaborent pas officieusement par quelques accords tacites ?
Depuis les révélations d'Edward Snowden et même avant, beaucoup se sont posés ces questions et se les posent encore, même avec les meilleures garanties de protection. Une garantie ne marche que par le crédit que vous accordez à celui ou celle qui la formule.
C'est la semaine prochaine que le projet de loi « Pouvoirs d'enquête » ou « investigatory power bill » (dont nous vous parlions la semaine dernière), que certains nomment déjà « loi espion », sera publiée et avec elle les nouveaux pouvoirs alloués aux services de sécurité du Royaume-Uni pour accéder aux données des suspects. Parmi eux, la possibilité pour les services secrets britanniques, après l'aval du ministère de l'Intérieur, de pirater le téléphone et/ou l'ordinateur d'un suspect pour récupérer l'ensemble des données transitant sur l'appareil, et ce, afin de contourner les méthodes de chiffrement des communications.
Liens : http://www.journaldugeek.com/2015/10/30/royaume-uni-renonce-backdoors-ou-presque/

Google, WhatsApp, Facebook et Snapchat accélèrent un peu plus sur le chiffrement

En pleine bataille entre Apple et le FBI autour du chiffrement, les géants du web ont non seulement apporté leur soutien à la firme à la pomme, mais entendent également renforcer le chiffrement des données utilisateurs.
Apple et le gouvernement se livrent une bataille sans précédent autour du chiffrement. Sans précédent par les enjeux en balance et le nombre d'acteurs concernés : gouvernements, agences de renseignement US et étrangères, citoyens du monde entier, entreprises high-tech, etc.
Dans cette bataille chacun choisit son camp et il n'a pas fallu bien longtemps aux géants du web pour se positionner derrière Apple contre le FBI, le gouvernement et même Barack Obama.
Présent au festival SXSW, le président américain, sans véritablement trancher sur la question, les a vivement incités à trouver rapidement une solution avant que le législateur ne s'empare de la question en édictant une loi « dangereuse ». Une menace

à peine voilée qui ne semble pas avoir trouvé l'écho espéré du côté de la Silicon Valley.
Alors que WhatsApp pourrait être la prochaine cible des autorités, le quotidien britannique *The Guardian* révèle que la seule réponse donnée est celle d'un renforcement du chiffrement proposé sur leurs services. Et par renforcement, il faut entendre, chiffrement de bout-en-bout (*end-to-end*) des communications, c'est-à-dire que seuls les utilisateurs détiendront la clé de chiffrement à même de déverrouiller leurs données. Même sur demande des autorités munies d'un mandat, il sera alors impossible pour ces firmes d'accéder à leurs requêtes.
Si certains à l'image de Whatsapp ou Google proposent déjà un chiffrement des communications, celui-ci devrait donc se trouver renforcé.
Du côté de Whatsapp, filiale de Facebook, on se dirigerait vers un chiffrement des appels vocaux et des discussions de groupe. Whatsapp pourrait faire une annonce en ce sens dans les semaines à venir. Quant à la maison mère, Facebook, elle pourrait se convertir et renforcer la sécurité de Messenger, son service de messagerie.
Du côté de Snapchat, les sources précisent que l'entreprise travaillerait également sur un service de messagerie sécurisée.
Chez Google, si le sujet est sur la table depuis 2014, les choses avancent lentement. En effet, le fonctionnement de Gmail est au cœur du problème. Google propose déjà à ses utilisateurs l'envoi d'emails chiffrés. Toutefois, le développement du chiffrement de bout-en-bout sur ses autres services pose question au regard de son modèle économique. La firme tentant d'allier les deux sans porter préjudice à l'un ou à l'autre.
Apple et Google n'ont pas les mêmes difficultés puisque les deux firmes n'ont pas le même *business model*. Google vend des publicités ciblées à partir des scans effectués sur les emails de ses utilisateurs. Un chiffrement de bout-en-bout empêcherait le robot de *lire* ce contenu.
Même dans la tourmente, la firme de Cupertino ne renonce pas à sécuriser un peu plus ses services. Récemment encore, Apple s'est attaché les services du développeur de Signal – la messagerie chiffrée plébiscitée par Edward Snowden – afin de venir renforcer les équipes sécurité d'iOS lors d'un stage d'été.
Cette course au chiffrement ne sera pas sans fin. Gageons que ces entreprises devront trouver une solution satisfaisante pour les autorités, sans pour autant renoncer au chiffrement des communications. Pour certains experts, le juste milieu serait de proposer ce type de chiffrement, tout en maintenant la possibilité pour les autorités d'accéder aux métadonnées, ces informations qui révèlent le destinataire et l'expéditeur d'un message ainsi que sa date et heure d'envoi ou encore les données de localisation. Un casse-tête qui semble néanmoins inévitable.
Dans le cas inverse, la *prophétie* de Barack Obama pourrait se réaliser plus tôt que prévu. 15 mars 2016
Liens : http://www.journaldugeek.com/2016/03/15/google-whatsapp-facebook-snapchat-chiffrement/

Telegram supprime des comptes de Daech

L'application chouchou des terroristes de l'Etat islamique s'est décidée à agir en supprimant plusieurs comptes liés à l'organisation.
Montré du doigt par la presse britannique et américaine dans la foulée des attentats pour être l'application de messagerie chiffrée favorite des membres de l'organisation

État islamique (OEI), leur permettant de communiquer en toute quiétude, Telegram semble enfin décidé à agir.
Si son fondateur et PDG, le libertarien Pavel Durov, s'est toujours illustré par son indépendance vis-à-vis de tout gouvernement, ne cédant à aucune demande d'accès aux données utilisateurs (informations et contenu), tenant tête aussi bien au Kremlin qu'à l'ran, il a consenti à quelques concessions. Ainsi, sans fournir la moindre information sur le contenu des messages présents sur sa plateforme, Telegram a procédé à un nettoyage des comptes liés à l'OEI, ou plutôt des salons publics ayant pignon sur rue.
Ainsi, Telegram a précisé sur Twitter que 78 chaines liées à l'OEI ont été bloquées et ce dans 12 langues, feignant de découvrir, horrifié, que l'OEI utilise l'application pour diffuser sa propagande. Ce n'est pourtant un secret pour personne, l'OEI elle-même en fait la promotion dans ses médias. Comme le rappelle *Le Monde*, c'est sur ce média que l'OEI a revendiqué les attentats du 13 novembre et celui perpétré contre l'avion russe à Charm el cheikh, dans le Sinaï.
« *Nous avons été très perturbés d'apprendre que les chaînes publiques de Telegram étaient utilisées à des fins de propagande djihadiste* », a ainsi expliqué l'app dans un communiqué. Et annonce dans la foulée la création prochaine d'un outil permettant de faciliter le signalement de contenus « *répréhensibles* ».
Reuters minimise cependant la portée d'un tel nettoyage puisque telle une hydre, l'organisation créée de nouveaux comptes lorsqu'elle constate que d'autres ont été fermés, comme on peut le voir également sur Twitter où un compte a été censuré plus de 300 fois.
Liens : http://www.journaldugeek.com/2015/11/19/telegram-supprime-comptes-deash-accuse-france/

Une proposition de loi CD&V pour assécher le financement de l'extrémisme

Le CD&V a rédigé une proposition de loi visant à octroyer à la Cellule de Traitement des Informations Financières (CTIF) les moyens d'examiner le financement d'activités extrémistes en lien avec les enquêtes sur le terrorisme.
Actuellement, «les extrémistes peuvent financer des bases de repli et des réseaux de soutien sans que la CTIF puisse intervenir», justifie l'auteur de la proposition, le député Veli Yüksel, interrogé dans le Tijd.
«Aujourd'hui, la CTIF ne peut intervenir qu'en cas de terrorisme et pas d'extrémisme, une situation qui fait craindre que l'on passe à côté de certaines affaires», précise le député, membre de la commission terrorisme.
Selon lui, «la CTIF doit jouer un rôle plus actif dans la lutte contre le terrorisme, aux côtés de la police et de la Justice». Il doit s'agir de «traquer le déploiement logistique des réseaux extrémistes à un stade plus avancé», poursuit-il, soulignant que la CTIF elle-même est demandeuse d'une telle évolution. Le député CD&V souhaite également un échange automatique entre le fisc et les banques, des données financières telles que les comptes en banque, les plus-values sur la vente d'actifs, les dividendes, etc. Ces informations doivent pouvoir servir d'éléments de preuve dans le cadre de la lutte contre le financement du terrorisme et du blanchiment d'argent.
Le parti socialiste avait déjà déposé une série de propositions de loi visant notamment à assécher le financement du terrorisme, estimant que le projet du gouvernement à cet égard avait manqué sa cible.

Liens : http://www.sudinfo.be/1621047/article/2016-07-12/une-proposition-de-loi-cdv-pour-assecher-le-financement-de-l-extremisme

Le Bitcoin dans la ligne de mire de Bruxelles

Dans le cadre d'un plan de lutte contre le financement du terrorisme, la Commission européenne a présenté diverses mesures contre l'évasion fiscale et le blanchiment d'argent. Parmi elles, certaines visent à mieux contrôler les monnaies virtuelles comme le Bitcoin et les cartes prépayées, notamment en supprimant l'anonymat qu'elles confèrent.

Autrefois ignorées et/ou mal appréhendées, les monnaies virtuelles intéressent désormais les gouvernements et politiques.

Dans le cadre d'un vaste plan de lutte contre le financement du terrorisme, la Commission européenne a présenté des mesures touchant directement les monnaies virtuelles et les cartes prépayées.

Le Bitcoin parce que la monnaie est notamment utilisée pour régler certains achats illicites sur Internet, de la drogue, aux faux papiers en passant par les armes et autres explosifs, et il a été prouvé que les auteurs des attentats de novembre 2015 à Paris ont utilisé des cartes prépayées pour communiquer. Ces deux outils ont également l'avantage, pour ceux qui les utilisent, d'être totalement anonymes.

L'objectif affiché par le premier vice-président de la Commission, M. Frans Timmermans, est donc de « *priver les terroristes des ressources qu'ils utilisent pour commettre leurs crimes odieux* ». « *En repérant et en tarissant les sources de financement des réseaux terroristes, nous pouvons réduire leur capacité à voyager, à acheter des armes et des explosifs, à planifier des attentats et à propager la haine et la peur sur la toile* ».

Pour se faire, plusieurs mesures ont été proposées visant à lever l'anonymat entourant ces outils afin d'identifier d'éventuelles cellules terroristes.

« La Commission propose d'inclure les plateformes de change de monnaies virtuelles dans le champ d'application de la directive anti-blanchiment, de manière à ce que ces plateformes doivent appliquer des mesures de vigilance à l'égard de la clientèle lors de l'échange de monnaies virtuelles contre des monnaies réelles, ce qui mettra fin à l'anonymat associé à ce type d'échange ».

Concernant les cartes prépayées, « *la Commission propose d'abaisser les seuils en dessous desquels une identification n'est pas requise et d'élargir les exigences relatives à la vérification de l'identité des clients. Il sera veillé à la proportionnalité de ces mesures, eu égard en particulier à l'utilisation de ces cartes par des citoyens vulnérables sur le plan financier* ». Concrètement, l'identification du détenteur d'une carte prépayée sera requise dès 150€, contre 250€ aujourd'hui.

À charge pour la Commission européenne de légiférer pour que ces mesures soient « *menées à bien pour la fin de 2017* ». Mesures qui devront être adoptées par le Conseil des États membres et le Parlement européen.

La Commission précise toutefois qu'elle veillera à ne pas pénaliser le citoyen lambda, utilisateur légitime de bitcoins et autres moyens de paiements anonymes.

12 juillet 2016

Liens : http://www.journaldugeek.com/2016/07/12/bitcoin-bruxelles/

Blanchiment des capitaux et financement du terrorisme: Environ 1500 milliards de dollars annuellement blanchis à l'échelle mondiale

Le blanchiment des capitaux et le financement du terrorisme sont intimement liés. Le phénomène a pris de l'ampleur dans le monde. Selon le président de la Cellule nationale de traitement des informations financières(CENTIF), M. Marimpa Samoura, le phénomène fait annuellement perdre plus de 1500 milliards de dollars à l'économie mondiale.

Le phénomène de blanchiment prend de l'ampleur dans le monde et constitue une source de déséquilibre économique. Et, à en croire le président du CENTIF, les montants annuellement blanchis sont estimés environ à 1500 milliards de dollars, soit 6 fois l'aide publique au développement.

La CENTIF, selon M. Marimpa Samoura, a reçu au total plus de 200 dossiers sur le blanchiment des capitaux. Et «sur ces dossiers, 23 ont été transmis à la justice pour, seulement 4 condamnations», regrette-t-il. Selon lui, le CENTIF n'a pas la compétence de révéler les noms des personnes impliquées dans le blanchiment de capitaux. «La CENTIF fait un travail confidentiel», a-t-il expliqué.

Au cours d'un atelier organisé pour la presse, M. Simpara a souligné que le blanchissement des capitaux et le financement du terrorisme sont intimement liés.

Mais, le phénomène est très mal perçu par le citoyen malien. C'est pourquoi la Cellule a organisé, jeudi 07 juillet 2016, un atelier en faveur des journalistes. «Le détournement de bien public, la corruption et l'évasion fiscale, constituent des sources de blanchiment dans un pays. Pour connaitre ce phénomène néfaste, il ya lieu d'imprégner les hommes de média sur les concepts de blanchiment», a déclaré d'entrée de jeu le président de la CENTIF, Marimpa Samoura.

Disposant d'une loi uniforme, une législation qui innove en fusionnant la lutte contre le blanchiment des capitaux et le terrorisme, le Mali est bien outillé pour faire face à ce phénomène. En plus de cette loi, M. Moumini Guindo (Secrétaire général du ministère de la Justice, des Droits de l'Homme et Garde des sceaux), indique que le Mali compte aujourd'hui 16 inspections judicaires, des structures de contrôle et le Bureau du vérificateur général.

L'inspecteur de police Soulamane Traoré, le magistrat Mamadou Kassogué et Mme Touré Aminata Dembélé étaient les experts désignés par la CENTIF pour animer cet atelier. Ils ont largement expliqué les concepts de base sur la lutte contre le blanchiment des capitaux et du financement du terrorisme.

Les experts ont donné un aperçu historique du phénomène et son évolution dans le temps et dans l'espace, les techniques et les stratégies adoptées par les criminels financiers, les dispositions juridiques nationales et internationales conçues pour faire face à cette menace grandissante qui perturbe les économies nationales et exposent les pays à une instabilité institutionnelle.

Les journalistes ont été également imprégnés des conséquences néfastes du blanchiment des produits du crime financier sur l'économie de manière générale ; des mesures dissuasives admises à titre préventif ; des sanctions prévues à l'effet de réprimer les contrevenants et de la nécessité impérieuse de la coopération et de la coordination entre les structures internes et externes chargées de la lutte contre le crime transnational organisé.

Au terme des travaux, les experts de la CENTIF et les journalistes ont dégagé des pistes de solutions pour mieux sensibiliser les citoyens sur l'ampleur du phénomène.
Pour ce faire, il a été convenu de porter sur les fonts baptismaux un réseau des journalistes pour la sensibilisation contre le blanchissement des capitaux et le financement du terrorisme. 13 Juillet 2016

Liens : http://malijet.com/actualite_economique_du_mali/160415-blanchiment-des-capitaux-et-financement-du-terrorisme-environ-15.html

Mali :
Le blanchiment des capitaux coûte 300 Milliards à l'Etat

Pour promouvoir la transparence financière et éradiquer le terrorisme, le gouvernement malien a crée un nouvel organisme dénommé CENTIF (Cellule Nationale de Traitement des Informations Financières). La CENTIF a organisé à l'endroit des hommes de medias, le jeudi 7 juillet, un atelier de formation et de sensibilisation sur le blanchiment des capitaux et le financement du terrorisme.
L'atelier, qui a eu à la Maison de la presse, était présidé par Moumouni Guindo, Secrétaire Général du ministère de la Justice, en présence de Marimpa Samoura, directeur de la CENTIF, et de Dramane Aliou Koné, président de la Maison de la presse. Au cours de la rencontre, il a été traité les concepts de lutte contre le blanchiment de capitaux et le financement du terrorisme; les techniques et stratégies utilisées par les criminels et les dispositions juridiques nationales et internationales conçues pour lutter contre ces fléaux.
Les conséquences néfastes du blanchiment de capitaux sur l'économie ont été expliquées. Selon Toure Aminata Dembélé, cadre de la BECEAO, le blanchiment de capitaux est le processus par lequel le produit du crime subit une série d'opérations visant à en dissimiler l'origine illicite et à lui donner une apparence licite.Quant au financement du terrorisme, il consiste à fournir des fonds dans l'intention de les voir utiliser dans des actes terroristes.
Au Mali, le blanchiment de capitaux et le financement du terrorisme existent. Selon Amadou Kassogué, juge d'instruction au pôle économique de Bamako, ces fléaux sont favorisés par le faible taux de bancarisation de l'économie et l'extrême pauvreté des populations. Souleymane Traoré, contrôleur général de police, estime, lui, que la CENTIF est une arme efficace de lutte contre le blanchiment des capitaux et le financement du terrorisme.
A ses dires, la CENTIF a pour missions le traitement et la transmission d'informations en vue de lutter contre le blanchiment des capitaux et le financement du terrorisme. « La CENTIF est la seule institution qui reçoit les déclarations de soupçons et peut demander d'investiguer n'importe quelle structure. Elle travaille avec des personnes susceptibles d'émettre des déclarations de soupçons: établissements financiers, hôtels, casinos, agences immobilières, particuliers, etc. »
A la fin des travaux, le président de la CENTIF, Marimpa Samoura, a sollicité la coopération de tous les citoyens et de la presse pour dénoncer des pratiques de blanchiment. Il a révélé qu'à cause du blanchiment d'argent, les cordons douaniers du Mali perdent 200 milliards par an et les impôts 100 milliards. 12 juillet 2016

Liens : http://maliactu.net/mali-le-blanchiment-des-capitaux-coute-300-milliards-a-letat/

Mali :
Lutte contre le blanchiment des capitaux et le financement du terrorisme

200 déclarations de soupçons reçues par la CENTIF 24 dossiers transmis à la justice, avec 4 condamnations

Le phénomène de blanchiment de capitaux et de financement du terrorisme a pris des proportions démesurées dans notre pays. Tenez-vous bien, depuis sa prise de fonction à la Cellule nationale de traitement des informations financières (CENTIF), il y a deux ans seulement, le Président de cette structure, l'ancien ministre Marimpa Samoura, a déjà reçu 200 déclarations de soupçon de blanchiment de capitaux et de financement terrorisme.

Sur lesquelles 24 dossiers ont été transmis à la justice, qui ont connu 4 condamnations lors de la dernière session des Assises de la Cour d'Appel de Bamako. Ces informations ont été données par le Président de la CENTIF lors de l'atelier de sensibilisation à l'intention des journalistes sur ces phénomènes, le 7 juillet dernier à la Maison de la presse.

Face à l'importance du fléau dans notre pays, le Président de la CENTIF a invité les populations à l'éveil des consciences et à avoir le courage de dénoncer les soupçons de blanchiment de capitaux et de financement du terrorisme. Selon lui, ce n'est pas égoïste que de dénoncer ceux qui font la fraude fiscale ou ceux qui se livrent à des détournements de deniers publics.

«Pour les Maliens, c'est normal qu'un agent des douanes ou qu'un travailleur des impôts puisse construire des maisons par ci et par là. Sur quelle base? Entre celui qui doit payer 10 millions d'impôt et qui s'arrange à payer seulement 2 ou 5 millions à l'Etat et celui qui le dénonce, qui est le plus égoïste?», s'est-il interrogé, appelant à l'éveil des consciences avant que le phénomène ne détruise notre économie.

Il également a relevé que le blanchiment ne se limitait pas à la vente de la drogue. Selon lui, le phénomène a gangréné tous les secteurs d'activité de notre pays. C'est pourquoi il a en a appelé à la vigilance afin de démasquer ces malfrats. D'où l'idée de ce partenariat qu'il a scellé avec la presse, pour informer et sensibiliser l'opinion sur ce danger qui mine notre société. Selon lui, en initiant cet atelier, il s'agissait d'imprégner les journalistes du concept de blanchiment.

«Comment comprendre que la Côte d'Ivoire et le Sénégal, plus industrialisés que le Mali, paient respectivement à l'UEMOA 30 et 15 milliards FCFA sur la base de leurs importations et que notre pays ne paie que 5 milliards de FCFA? Cela veut dire que notre pays importe moins que ces deux pays. Il y a quelque chose qui ne va pas. Nous devons tous prendre notre responsabilité et agir», a-t-il déclaré.

Rappelons que la CENTIF a pour mission le traitement et la transmission d'informations en vue de la lutte contre le blanchiment de capitaux et le financement du terrorisme. A ce titre, elle «est chargée notamment de recueillir, d'analyser, d'enrichir et d'exploiter tout renseignement propre à établir l'origine ou la destination des sommes ou la nature des opérations ayant fait l'objet d'une déclaration ou d'une information reçue, au titre des dispositions des articles 15, 36, 43, 70, 79, 80, 86 et 111 de la Loi sur le blanchiment de capitaux et le financement du terrorisme, reçoit également toutes autres informations utiles nécessaires à l'accomplissement de sa mission, notamment celles communiquées par les autorités de contrôle ainsi que les officiers de police judiciaire, qu'elle traite, le cas échéant, comme en matière de

déclaration d'opération suspecte, peut demander la communication, par les assujettis ainsi que par toute personne physique ou morale, d'informations détenues par eux et susceptibles de permettre d'enrichir les déclarations de soupçons».

La CENTIF est la seule structure habilitée à recevoir les déclarations de soupçon au Mali. On ne peut lui opposer le secret professionnel dans l'exercice de ses missions. Elle doit en retour garantir la confidentialité des informations qu'elle reçoit des assujettis. Elle traite et analyse immédiatement les informations recueillies et procède, le cas échéant, à des demandes de renseignements complémentaires auprès du déclarant, des autres assujettis, des Cellules de Renseignement Financiers étrangères ainsi que de toute autorité publique et / ou de contrôle.

Lorsque ses investigations mettent en évidence des faits susceptibles de relever du blanchiment du produit d'une activité criminelle ou du financement du terrorisme, la CENTIF saisit le Procureur de la République. C'est ce sens qu'elle a déjà transmis à la justice 24 dossiers, sur lesquels il y a déjà eu 4 condamnations à des peines diverses.

Liens : http://maliactu.net/mali-lutte-contre-le-blanchiment-des-capitaux-et-le-financement-du-terrorisme-200-declarations-de-soupcons-recues-par-la-centif-24-dossiers-transmis-a-la-justice-avec-4-condamnations-2/