CTRF CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER خلية معالجة الإستعلام المالي CTRF

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

Lettre n°95

UE : de nouvelles mesures de lutte contre le financement du terrorisme

La Commission européenne propose une directive visant à combattre le blanchiment de capitaux grâce au droit pénal, un règlement relatif aux contrôles de l'argent liquide et un règlement relatif à la reconnaissance mutuelle des décisions de gel et de confiscation d'avoirs d'origine criminelle.

Dans le cadre des engagements de son plan d'action destiné à renforcer la lutte contre le financement du terrorisme présenté en février 2016, la Commission a adopté le 21 décembre 2016 un train de mesures visant à renforcer la capacité de l'Union à combattre le financement du terrorisme et la criminalité organisée.

Une proposition de directive visant à combattre le blanchiment de capitaux grâce au droit pénal prévoit :

- des règles minimales relatives à la définition des infractions et des sanctions pénales liées au blanchiment de capitaux et un comblement des écarts entre les règles nationales pour empêcher l'exploitation de ces différences à des fins criminelles ;
- la suppression des obstacles à la coopération judiciaire et policière transfrontière en mettant en œuvre des dispositions communes pour améliorer les enquêtes concernant les infractions liées au blanchiment de capitaux ;
- l'alignement des normes de l'Union sur les obligations internationales dans ce domaine, énoncées dans la convention de Varsovie du Conseil de l'Europe et les recommandations du groupe d'action financière (GAFI).

Afin de fournir aux autorités compétentes les outils appropriés pour détecter les terroristes et leurs soutiens financiers, un règlement relatif aux contrôles de l'argent liquide vise à :

- renforcer le contrôle des mouvements d'argent liquide en ce qui concerne les personnes entrant dans l'UE ou qui en sortent avec 10.000 € ou plus en espèces ;
- permettre aux autorités d'agir même lorsque les montants concernés sont inférieurs au seuil de 10.000 € prévu pour la déclaration en douane, lorsqu'elles soupçonnent une activité criminelle ;
- améliorer l'échange d'informations entre autorités et Etats membres ;
- étendre les contrôles douaniers aux envois d'argent liquide par colis postal ou par fret ainsi qu'aux matières précieuses telles que l'or, qui ne sont actuellement pas couvertes par la déclaration douanière standard.

Enfin, une proposition de règlement relatif à la reconnaissance mutuelle des décisions de gel et de confiscation d'avoirs d'origine criminelle permettra de:

- disposer d'un instrument juridique unique pour la reconnaissance tant des décisions de gel que des décisions de confiscation dans les autres États membres de l'UE, simplifiant ainsi le cadre juridique existant ;
- élargir la portée des règles actuelles relatives à la reconnaissance transfrontière à la confiscation des avoirs de tiers ayant un lien avec le criminel ;
- améliorer la rapidité et l'efficacité des décisions de gel ou de confiscation grâce à un document standard et à l'obligation des autorités compétentes de communiquer entre elles ;

- assurer le respect des droits à réparation et à restitution en faveur des victimes. victime prime celui de l'Etat d'exécution et d'émission.
http://www.lemondeduchiffre.fr/le-magazine-de-la-profession-comptable/unes/280060-ue-de-nouvelles-mesures-de-lutte-contre-le-financement-du-terrorisme.html

La création d'un Centre européen contre-terrorisme : Vers l'amélioration du partage de renseignements ?

Depuis les derniers attentats de Paris, le 13 novembre dernier, l'Europe doit faire face à une menace terroriste accrue. La dimension inédite et internationale de l'État islamique appelle l'Union à développer de nouveaux outils efficaces pour lutter contre le terrorisme. L'urgence de la situation européenne et la nécessité de « *renforcer notre réponse à la terreur* » a permis d'accélérer l'ouverture d'un véritable Centre européen de contre-terrorisme (CECT) au sein d'Europol, inauguré le lundi 25 janvier à La Haye. Il est absolument nécessaire de permettre un partage optimal des informations entre les différents États membres, car il est certain que les derniers événements tragiques ont montré les lacunes de l'Union européenne dans le domaine.

Europol est l'office européen des polices. Cet organisme est alors chargé de renforcer et d'améliorer la coopération et l'échange de renseignements entre les autorités policières des États membres, en vue de lutter contre la criminalité internationale. La création du CECT fait suite au Conseil JAI (justice et affaires intérieures) du 20 novembre dernier portant sur le renforcement de la réponse pénale à la radicalisation conduisant au terrorisme et à l'extrémisme violent. Le Conseil a prévu le lancement du Centre européen de lutte contre le terrorisme, avant tout avec l'objectif de créer une « *plateforme permettant aux États membres de renforcer l'échange d'informations et la coopération opérationnelle en ce qui concerne la surveillance des combattants terroristes étrangers et les enquêtes à leur sujet, le trafic d'armes illicites et le financement du terrorisme* ».

Ce nouveau Centre a d'ores et déjà son directeur, comme le précise le communiqué de presse d'Europol en date du 25 janvier dernier. Il s'agit de M. Manuel Navarrete Paniagua, un haut officier de la Guardia Civil espagnole, disposant d'une longue expérience dans le domaine de la lutte anti-terroriste, puisqu'il était déjà chef d'unité dans le domaine au sein d'Europol. Le CECT compte également 39 membres et 5 experts nationaux.

La visée d'Europol va alors être de fournir aux États membres, ainsi qu'à ses partenaires tels que Interpol et Eurojust, de nouveaux moyens pour lutter plus efficacement contre le terrorisme en vue de l'amélioration de la coopération européenne grâce notamment à :

- L'accroissement de l'échange d'informations sur les données sensibles concernant la menace terroriste.
- La possibilité de détacher des experts du CECT en vue d'apporter un soutien dans les enquêtes transfrontalières, dans le but de garantir des réponses rapides et complètes en cas de nouvelles attaques terroristes.

La nécessité d'une amélioration de l'échange de renseignements entre les autorités policières est au cœur du débat contre le terrorisme, nous avons encore pu en être témoins lors de l'assemblée plénière du Parlement européen le 21 janvier dernier. C'est l'une des clefs face à la menace terroriste grandissante et transfrontalière que nous sommes en train d'affronter.

Il existait déjà, depuis 2010, un centre international de lutte contre le terrorisme, situé également à La Haye. C'est alors un « *organisme indépendant chargé d'étudier les aspects juridiques de la lutte contre le terrorisme, de formuler des recommandations à cet égard et d'identifier les meilleures pratiques en matière de prévention du terrorisme* ». Mais il s'agit avant tout d'un institut de recherche visant à examiner les aspects juridiques de la lutte contre

le terrorisme et à analyser les différentes mesures préventives prises à cet effet. Ses travaux peuvent d'ailleurs servir d'appui à la coopération entre les États membres de l'Union. Mais il semblait nécessaire de créer un centre européen dédié à la lutte contre le terrorisme, non pas en tant que centre de recherche, mais véritablement comme un outil d'amélioration du partage des renseignements, et nécessairement, de la coopération.

La sécurité avant tout, il est nécessaire de disposer de moyens d'action efficaces, et il va de soi qu'une amélioration des échanges d'informations entre les États membres est l'une des conditions *sine qua non* pour la lutte contre le terrorisme. Il s'agit de s'adapter, avec des moyens plus européens, à cette nouvelle menace. La coopération des États membres et d'Europol permettra alors de réunir les informations les plus pertinentes en vues d'appréhender les possibles acteurs de l'État islamique afin d'éviter, le mieux possible, de nouveaux drames.

Si le CECT était prévu depuis plusieurs mois, et n'est donc pas directement lié aux attentats de Paris, ces derniers ont tout de même permis de se rendre compte que le système européen connaissait de véritable failles, et un meilleur échange d'informations entre la France et la Belgique, notamment, aurait permis une appréhension plus efficace des suspects. Ce centre opérationnel permanent devrait pouvoir aider les autorités policières à combattre la criminalité internationale. Il est nécessaire, comme l'a notamment indiqué le premier vice-président de la Commission européenne, Frans Timmermans, que les États européens soient en mesure de « *travailler ensemble en confiance* ». Grâce à un partage accru des renseignements, les États seront plus à même de « *traquer les financements terroristes* » notamment, a déclaré le directeur d'Europol, Rob Wainwright. Afin de vaincre le terrorisme, qui ne connaît pas de frontières, l'Union doit, plus que jamais, former un espace européen soudé.

Il est clair qu'actuellement, au sein de l'espace de liberté, de sécurité et de justice, l'accent est mis sur la sécurité, peut être au détriment des deux autres composantes de cet espace européen, face à la nécessité d'une réponse à la terreur qu'essaie de mettre en place l'État islamique au sein de notre société occidentale. Si l'échange et le partage d'informations sont une nécessité face à la menace terroriste, certains parlementaires européens ont fait remarquer qu'il ne fallait pas pour autant commencer à collecter « *un tas d'informations qui ne servent pas* » (Jan-Philipp Albrecht). Le but est d'améliorer la lutte efficace contre Daesh, pas de se noyer sous une multitudes d'informations provenant des 28 États membres sans que cela ne soit d'une grande aide. Il faut réussir à collecter les informations pertinentes, afin de pouvoir prévenir de nouveaux attentats. Le CECT semble être un moyen efficace pour cela, si, et seulement si, les États acceptent véritablement de coopérer

https://europe-liberte-securite-justice.org/2016/02/02/la-creation-dun-centre-europeen-contre-terrorisme-vers-lamelioration-du-partage-de-renseignements/

Les implications informatiques de la dernière loi de lutte contre le terrorisme

De la consécration du concept de vol de données à l'extension du filtrage administratif d'Internet, la récente loi va bien au-delà de la seule lutte contre le terrorisme.

Depuis le 11 septembre 2001, l'usage que les organisations terroristes peuvent faire de l'internet préoccupe les pouvoirs publics. 2014 a été marquée par les révélations sur le prosélytisme djihadiste qui peut se développer sur les réseaux sociaux. Internet est donc un enjeu de sécurité publique à différents titres : il est tout à la fois une source de contenus délictueux - contre la propagation desquels les pouvoirs publics entendent lutter - et un moyen d'investigation à la disposition des autorités de police.

L'arsenal législatif en la matière ne cesse de se développer et de se complexifier. Les lois sur le sujet se succèdent avec une belle régularité : la loi du 15 novembre 2001 relative à la sécurité quotidienne, loi du 23 janvier 2006 relative à la lutte contre le terrorisme, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, sont toutes venues modifier le code de procédure pénal pour intégrer ce média bien particulier qu'est internet.

Le dernier texte en date est la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme. Si ce texte comprend de nombreuses dispositions sans rapport avec internet, plusieurs articles concernent le réseau et plus généralement les systèmes d'information.

Le filtrage de l'internet pour lutter contre l'apologie et la provocation au terrorisme

Le législateur français flirte depuis longtemps avec la volonté de trouver dans les FAI le relais efficace de la lutte contre les contenus illicites que véhicule l'internet, particulièrement la pédopornographie et le terrorisme. Mais le blocage de sites internet sur simple décision administrative et sans décision préalable d'un juge suscite des réserves logiques dans une société démocratique où la liberté de communication et d'expression doit être garantie.

C'est la loi relative aux jeux en ligne du 12 mai 2010 qui a initié le processus. Celle-ci prévoit que le président de l'autorité de régulation des jeux en ligne (ARJEL) peut saisir le président du tribunal de grande instance de Paris afin qu'il soit ordonné aux FAI de bloquer l'accès aux sites de jeux en ligne non autorisés en France. 49 sites ont déjà été bloqués.

La LOPPSI 2 du 14 mars 2011 a ensuite instauré la possibilité pour l'autorité administrative d'enjoindre aux FAI de bloquer l'accès aux sites pédopornographiques (article 6-I 7 de la loi du 21 juin 2004 tel que modifié par la loi du 14 mars 2011). Mais cette faculté, bien que validée par le Conseil constitutionnel dans sa décision du 10 octobre 2011, est à l'origine de nombreuses résistances, parmi lesquelles celle des FAI qui pointent la relative inefficacité du filtrage et son coût, mais également celle du Gouvernement lui-même ! En effet, le décret d'application nécessaire à l'effectivité de l'article 6-I 7 a été enterré par le Gouvernement...

L'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique est aujourd'hui complété d'un article 6-I qui prévoit un dispositif de filtrage applicable tant en matière de terrorisme que de pédopornographie.

L'autorité administrative doit d'abord demander à l'éditeur du contenu ou à l'hébergeur du site de retirer les contenus en cause. Elle en informe simultanément les FAI. En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux FAI la liste des « adresses électroniques des services de communication au public en ligne », comprendre les URL, des pages qui doivent être bloquées. Les FAI doivent alors empêcher sans délai l'accès à ces adresses.

Lorsque l'éditeur du site en cause n'est pas identifiable conformément à la loi française, ce qui sera pour ainsi dire toujours le cas car ces sites sont rarement hébergés en France, l'administration peut demander directement aux FAI le filtrage, sans notification préalable à l'éditeur.

Dans le but honorable d'instaurer une forme de contrôle à cette « censure » de l'internet, le législateur a prévu que les demandes de retrait devront être transmises à une « personnalité qualifiée », désignée en son sein par la CNIL. Ce « sage » a la mission de s'assurer « de la régularité des demandes de retrait ». S'il constate une irrégularité, il peut à tout moment recommander à l'autorité administrative de mettre fin au filtrage. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée pourra saisir la juridiction administrative compétente, en référé ou sur requête.

Il s'agit donc de remettre le juge dans la boucle du contrôle du filtrage... mais sans le remettre tout à fait.
Les FAI ne sont pas les seuls acteurs de l'internet convoqués à la lutte contre la diffusion des messages terroristes et pédopornographiques : les moteurs de recherche peuvent également se voir notifier, selon la même procédure, des URL à déréférencer.
Last, but not least... les modalités d'application de cette procédure seront précisées par décret, notamment la compensation des surcoûts justifiés résultant des obligations mises à la charge des opérateurs. Si ce décret est aussi long à venir que celui précédemment attendu de la LOPPSI 2, au-delà des effets d'annonce, le dispositif restera lettre morte.

Renforcement des moyens d'investigations pour la police judiciaire

La nouvelle loi vient compléter les pouvoirs de perquisition des OPJ sur les systèmes informatiques.
La loi du 18 mars 2003 pour la sécurité intérieure a conféré aux officiers de police judiciaire et, sous leur responsabilité, aux agents de police judiciaire le droit d'accéder aux systèmes informatiques implantés sur les lieux où se déroule une perquisition. Ce faisant, OPJ et APJ peuvent accéder aux données stockées dans lesdits systèmes mais aussi dans un autre système informatique, dès lors que celui-ci est accessible à distance à partir du système initial.
Ce dispositif présentait la contrainte pour les OPJ de devoir effectuer leurs investigations sur le système d'instant dans les locaux mêmes où se déroule la perquisition. Le nouvel article 57-1 du Code de procédure pénal permet maintenant aux enquêteurs d'accéder au système « distant » depuis les locaux de leurs propres services disposant ainsi des conditions optimales pour recueillir et exploiter les données. Il s'agit donc d'une forme de « perquisition » à distance.
L'article 19 de la nouvelle loi étend également le champ d'application des enquêtes dites « sous pseudonyme ». La loi a ponctuellement permis à des agents spécifiquement habilités d'enquêter en ligne, sous pseudonyme, afin de recueillir des preuves d'infractions commises sur ou par l'intermédiaire du réseau. Les enquêteurs sont alors irresponsables pénalement et peuvent ainsi échanger des contenus illicites avec les personnes qui sont la cible de leurs investigations. Toutefois, les enquêteurs ne doivent pas inciter à la commission d'un délit ou d'un crime. La possibilité de réaliser des enquêtes en ligne sous pseudonyme est maintenant étendue à l'ensemble des délits et crimes relevant de la criminalité organisée.

Le vol de données informatiques consacré

L'infraction pénale qui protège principalement la propriété est le vol, ainsi défini par l'article 311-1 du code pénal : « Le vol est la soustraction frauduleuse de la chose d'autrui ». Le substantif « chose » est-il suffisamment accueillant pour rendre compte de la soustraction d'un élément incorporel comme des données ou une information ?
La jurisprudence de la cour de cassation était encore à ce jour hésitante sur cette question. Lorsque la soustraction de l'information s'opère pas le biais de la soustraction d'un bien corporel, qui en est le support, la jurisprudence a confirmé depuis longtemps que l'on était bien en présence de l'élément matériel du vol. Après le vol par photocopie, la cour de cassation a reconnu le vol par reproduction de disquettes. La cour de cassation a enfin reconnu le vol d'information, sans reproduction, dans le fait qu'un salarié ait permis à un tiers concurrent de prendre connaissance, à son domicile, de documents de l'entreprise qui l'embauche. Un nouveau pas vers le vol d'informations avait été franchi par la cour de cassation dans un arrêt du 4 mars 2008. Dans cette espèce, le vol de fichiers informatiques avait été réalisé par copie des fichiers sur support Syquest depuis le serveur où ils étaient stockés. A aucun moment le détenteur légitime des fichiers n'avait été dépossédé, même temporairement, desdits fichiers, y compris pendant le temps des opérations de reproduction.
L'évolution vers la reconnaissance du « vol » de données vient de se terminer avec la loi du 13 novembre 2014 et la modification qu'elle apporte à l'article 323-3 du code pénal. L'infraction

consacrée ne figure pas dans les dispositions du code relatives au vol mais a été intégrée dans le chapitre relatif aux diverses atteintes aux systèmes d'information.
L'article 323-3 punissait notamment le fait de « supprimer » ou de « modifier » frauduleusement les données d'un système d'information. Aux actions réprimées, la loi vient d'ajouter le fait « d'extraire, de détenir, de reproduire et de transmettre frauduleusement » ces données. Ainsi, l'appropriation frauduleuse d'une donnée informatique devient maintenant indubitablement un délit puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
http://www.cio-online.com/actualites/lire-les-implications-informatiques-de-la-derniere-loi-de-lutte-contre-le-terrorisme-7210.html

L'importance des nouvelles technologies dans la lutte contre le terrorisme

Et si les nouvelles technologies étaient le moyen clé permettant aux autorités étatiques de prévenir les actes de terrorisme ? Et s'il était possible de connaitre les intentions d'un individu en observant son historique de consultation de sites internet ? Quand les nouvelles technologies sont utilisées pour tenter de devancer les attaques terroristes…
Le 3 juin 2016, le parlement français a adopté la loi Urvoas ayant pour objet de « *renforcer la lutte contre le crime organisé, le terrorisme et leur financement* », mais également d' « *améliorer l'efficacité et les garanties de la procédure pénale* ». Cette loi introduit deux nouvelles incriminations dans le code pénal français, plus faciles à mettre en oeuvre que l'article 421-2-6, I 2° (c), qui exigeait alors la démonstration de la participation active de l'individu à un réseau terroriste. Preuve difficile à démontrer…
La première incrimination concerne la consultation répétée de sites djihadistes, punie de deux ans d'emprisonnement et de 30 000 euros d'amende (article 421-2-5-2 du code pénal). Cependant trois exceptions sont prévues, lorsque « la consultation :

- est effectuée de bonne foi ;
- résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ;
- intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice ».

Les preuves de consultation de ces sites sont produites de deux manières :

- soit grâce aux mouchards installés par les services de renseignement ou la police judiciaire sur les équipements informatiques des suspects ;
- soit par la consultation de l'historique sur les appareils saisis lors des différentes perquisitions.

La deuxième incrimination concerne l'incitation au terrorisme ou l'apologie du terrorisme. Elle est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende (article 421-2-5-1 du code pénal).
Il n'aura pas fallu plus de deux mois pour que cette loi fasse l'objet d'une application concrète. Le 8 aout 2016, le Tribunal correctionnel de Chartes a condamné à deux ans d'emprisonnement ferme, un homme de 31 ans, pour avoir consulté à plusieurs reprises des sites faisant l'apologie du terrorisme et incitant à commettre des attentats. La consultation de sites djihadistes s'est accompagnée d'autres éléments suspects comme par exemple le visionnage de vidéos de décapitations, mais également un post Facebook dans lequel l'individu avait publié une photo de la Tour Montparnasse en indiquant « *Montparnasse, quelle belle tour ?! On va lui rendre sa splendeur. Inch'Allah* ». Ou encore la recherche sur internet d'un moyen de se procurer des armes.

Autant d'éléments qui ont permis aux autorités judiciaires d'évaluer sa dangerosité et ainsi de le condamner. Dans cette toute première application concrète de la loi Urvoas il est possible de voir le rôle prépondérant des nouvelles technologies dans l'appréhension des délits liés au terrorisme. Dans cette affaire, la consultation des sites djihadistes a permis d'alerter les enquêteurs sur le profil de cet homme et de réunir assez d'éléments pour laisser penser que ce dernier était prêt à agir d'une façon ou d'une autre, soit en partant en Syrie faire le djihad, soit en commettant un attentat. Toutes les preuves de sa radicalisation ont donc été apportées grâce à des outils technologiques (ordinateur, téléphone cellulaire) ou à des réseaux sociaux.

Une autre condamnation a été prononcée, le 15 septembre dernier par le Tribunal correctionnel de Marseille. Un homme de 28 ans a été condamné à deux ans de prison ferme pour avoir consulté à 143 reprises, depuis une bibliothèque municipale, des sites internet diffusant la propagande menée par Daech. Interpellé alors qu'il cherchait sur internet un moyen de rejoindre la Libye, l'homme en question était surveillé par les services de renseignement français depuis un an. Il s'est avéré que son téléphone cellulaire contenait plus d'une centaine de vidéos de propagande.

Pour sa défense, ce dernier a tenté de soulever une des exceptions prévues par l'article 421-2-5-2 du code pénal en invoquant le moyen selon lequel il était « apprenti journaliste », ce qui a été écarté par les juges du fond.

L'aide des nouvelles technologies dans cette lutte ne s'arrête pas là. Cette fois-ci, c'est vers les applications de messagerie que les autorités se sont tournées pour prévenir des actes de terrorisme mais plus particulièrement Telegram, une des applications dans le viseur des enquêteurs depuis déjà quelques mois.

Créée en 2013 par les frères Nikolai et Pavel Durov, celle-ci permet d'assurer à chaque utilisateur la confidentialité accrue de ses données personnelles et la sécurité de ses échanges (suppression automatique des échanges au bout de quelques minutes). L'application assure être « *plus sûre que les autres applications de messagerie grand public* » et est par conséquent, très prisée des réseaux djihadistes.

Pour la première fois, un jeune homme de 29 ans a été condamné le 30 septembre dernier, par le Tribunal correctionnel de Paris, à quatre ans de prison, dont deux avec sursis. Il lui est reproché d'avoir entrainé un de ses correspondants à commettre un attentat sur le sol français, et un autre à partir faire le djihad en Syrie via cette application. Il a également été condamné pour avoir consulté des sites internet faisant l'apologie ou incitant au terrorisme. En effet, ce dernier était abonné à la chaine Telegram du groupe djihadiste Etat islamique et avait téléchargé des vidéos de propagande.

Le même jour, un collégien de 15 ans, inconnu jusqu'alors des services de renseignement, a été mis en examen et écroué. En effet, le mineur était en contact sur Telegram avec un djihadiste français soupçonné d'avoir téléguidé à distance les attaques de Magnanville (mort d'un policier et sa compagne), de Saint-Etienne-du-Rouvray (mort d'un prêtre) mais également d'être à la tête du commando de femmes démantelé début septembre en Essonne, après la découverte d'une voiture remplie de bonbonnes de gaz à Paris.

La multiplicité des cas récents ayant permis au juge d'appliquer la loi Urvoas permet de mieux comprendre l'importance des nouvelles technologies et plus particulièrement des réseaux sociaux dans la propagande menée par l'Etat islamique auprès des jeunes français. Ainsi il est primordial pour les autorités judiciaires d'utiliser ces nouveaux moyens de communication pour devancer toute tentative terroriste.

Les nouvelles technologies sont donc un point d'ancrage indispensable dans cette lutte, comme l'a rappelé le Procureur de la République de Nice, après les attentats qui ont ensanglanté la ville le 14 juillet dernier.

En effet, l'Etat islamique a fait des nouvelles technologies, « *une force paramilitaire* » comme le souligne Claude Sarrazin, président de SIRCO (entreprise québécoise spécialisée

dans les services de sécurité), dans une interview pour TVA Nouvelles, chaine de télévision québécoise. « *Ils ont une capacité informatique importante, des spécialistes en matière de web, utilisation des réseaux sociaux* » précise-t-il.
Cependant, le nouveau délit de consultation des sites internet djihadistes est déjà largement contesté par les défenseurs des droits. D'après Sami Khankan, avocat au Barreau de Nantes, deux problèmes ressortent de ce texte législatif. D'abord, le flou de l'exception posée à l'alinéa 2 de l'article 421-2-5-2 du code pénal mais également l'amoindrissement apportée à la liberté de communication. Il a déposé une question prioritaire de constitutionnalité (QPC), transmise le 14 septembre dernier par les juges du fond à la Cour de Cassation, première étape du processus légal de la QPC. Celui-ci estime que l'interdiction de consulter des sites « faisant l'apologie du terrorisme » serait contraire à la Déclaration Universelle des Droits de l'Homme et du Citoyen de 1789. Selon lui, il s'agirait d'une « atteinte à la liberté de communication et d'opinion ». Il soulève également dans ses moyens, que l'article du Code pénal est inconstitutionnel dans la mesure où il crée une « présomption de mauvaise foi » ainsi qu'une « rupture d'égalité » entre les citoyens puisque certains individus bénéficieraient d'une dérogation.
Pour Philippe Bas (sénateur et président de la commission des lois du Sénat) « c'est un élément important de la lutte contre le terrorisme » et « ce n'est pas innocent de consulter habituellement des sites qui appellent au meurtre ». En effet, dans une interview accordée à radio France culture, il considère qu'il s'agit de « l'antichambre du terrorisme ».
Malgré les contestations actuelles des nouvelles incriminations, il est évident que pour être efficace, les autorités étatiques ont été dans l'obligation d'adapter le cadre législatif au développement des nouveaux moyens de télécommunication pour en faire un élément stratégique de sa lutte contre le terrorisme.
http://droitdu.net/2016/10/limportance-des-nouvelles-technologies-dans-la-lutte-contre-le-terrorisme/

Bruxelles veut assécher le financement du terrorisme en surveillant bitcoins et cartes prépayées

La Commission européenne a présenté hier un « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* ». Plusieurs volets sont au programme, mais Bruxelles s'attarde particulièrement sur l'utilisation de moyens de paiement anonymes. Crypto-monnaies, cartes de paiement prépayées et espèces sont ainsi visées.
Alors qu'en France, l'état d'urgence est toujours d'actualité, près de trois mois après les attentats de Paris, la Commission européenne cherche des moyens de lutter contre le terrorisme. L'objectif pour les autorités européennes est de couper le robinet du financement des organisations terroristes, grâce à une série de mesures dont la mise en application s'étalerait sur 2016 et 2017.

Surveiller les plateformes d'échange de crypto-monnaies

Pour parvenir à cet objectif, Bruxelles voudrait agir simultanément sur plusieurs leviers. Outre le renforcement de la vigilance concernant « *les flux financiers en provenance de pays tiers à risque* » la Commission aimerait garder un œil sur « *les risques de financement du terrorisme, liés aux monnaies virtuelles* ».
Les crypto-monnaies permettent en effet d'effectuer des transactions financières de manière quasi instantanée d'un bout du monde à l'autre, dans un anonymat relatif. Si la Commission ne peut agir directement sur ces flux, elle peut cependant aller frapper à la porte des plateformes de change proposant de troquer ses bitcoins contre des euros, des dollars ou toute autre monnaie classique.

Bruxelles propose ainsi dans son « *plan d'action destiné à renforcer la lutte contre le financement du terrorisme* » d'inclure les plateformes de change de crypto-monnaies 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* ». L'objectif affiché des autorités est de « *mettre fin à l'anonymat associé à ce type d'échange* » d'ici « *la fin du deuxième trimestre* ».
En France, les plateformes d'échange doivent déjà se déclarer auprès de l'ACPR. Le Rapport Tracfin sur les crypto-monnaies publié en juillet 2014 suggérait déjà quant à lui la nécessité d'identifier les clients de ces plateformes, à partir du moment où ils effectuent des échanges entre euros et monnaies virtuelles.

Pas de bannissement des crypto-monnaies

Si Bruxelles souhaite réguler les échanges entre crypto-monnaies et monnaies fiduciaires, il n'est pas prévu de bannir leur utilisation. Si les plateformes d'échange seront soumises à de nouvelles obligations, via la quatrième directive anti-blanchiment, les fournisseurs de portefeuilles numériques pour les monnaies virtuelles (type Electrum, MultiBit) ne devraient quant à eux pas avoir à changer leurs habitudes.
Cependant, la Commission note que les monnaies virtuelles « *sont souvent considérées comme un outil intéressant pour les transferts internationaux d'argent* » et qu'elles « *représentent un marché innovant mais petit* ». Elle rappelle également que la Banque centrale européenne (BCE) avait jugé qu'elles ne représentaient pas une menace du point de vue de la stabilité financière de la zone euro. Aucune raison donc d'interdire leur utilisation, pour le moment.

Les cartes de paiement prépayées dans le collimateur de l'Europe

Bruxelles veut aussi « *s'attaquer aux risques liés aux instruments prépayés anonymes* », type TransCash ou PCS, qui permettent à n'importe qui de profiter d'une solution de paiement avec un plafond de 2 500 euros par carte, sans vérification d'identité au moment de l'ouverture du service. Ce type de carte ont notamment été utilisées pour la préparation des attentats de Paris, note la Commission Européenne dans une FAQ.
Les mesures autour de ces cartes n'ont pas encore été précisées, mais l'Europe voudrait abaisser le plafond à partir duquel il devient nécessaire de vérifier l'identité du futur détenteur de la carte avant de lui fournir le service. La Commission précise « *qu'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* ». Là encore, il est question d'une application d'ici mi-2016.
Les solutions de type Compte Nickel ne devraient quant à elles pas subir de contrecoup particulier, puisqu'elles nécessitent déjà une vérification de l'identité du client avant même l'ouverture du service.

Les espèces posent également problème

Il y a un dernier mode de paiement anonyme qui pose problème à Bruxelles et des centaines de millions de citoyens l'utilisent quotidiennement : les espèces. Intraçables elles sont pourtant omniprésentes dans la vie courante et il est encore impensable de les faire disparaître.
L'Europe voudrait néanmoins émettre une *« proposition législative relative aux mouvements illicites d'argent liquide », dans laquelle la Commission « étendra le champ d'application du règlement existant afin d'y inclure l'argent liquide envoyé par fret ou par la poste et de permettre aux autorités d'agir à l'égard de montants plus faibles d'argent liquide en cas de soupçons d'activité illicite ».*
On rappellera que le plafond pour les achats en espèces est passé de 3 000 à 1 000 euros en France le 1er septembre dernier, et que depuis le 1er janvier, les français doivent présenter une pièce d'identité pour toute opération de change d'une valeur de plus de 1 000 euros.

Depuis le 1er janvier, les banques doivent également signaler à Tracfin tout dépôt ou retrait d'espèces d'un montant supérieur à 10 000 euros par mois.

Le cas épineux du billet de 500 euros

La Commission, la Banque centrale européenne et Europol vont également travailler de concert pour évaluer la nécessité d'un retrait de la circulation des billets de 500 euros. Ceux-ci représentent un tiers de la valeur de l'ensemble des billets en circulation, alors même qu'ils ne sont que très peu utilisés lors de paiements.

« *Ces billets sont très demandés au sein des groupes criminels qui s'en servent pour transporter leur argent, en raison de leur grande valeur et de leur faible volume* ». Il est en effet plus facile de transporter clandestinement un seul billet de 500 euros qu'une liasse de 50 billets de 10 euros. Il reste encore à voir si cette mesure sera vraiment efficace, les billets de 100 et 200 euros n'étant pas beaucoup plus difficiles à camoufler.

https://www.nextinpact.com/news/98359-bruxelles-veut-assecher-financement-terrorisme-en-surveillant-bitcoins-et-cartes-prepayees.htm

La technologie au service de la lutte contre le financement du terrorisme

Logos IT Services, éditeur de la solution iDETECT, entame une nouvelle collaboration avec l'Université du Luxembourg et son Interdisciplinary Centre for Security, Reliability and Trust (SnT). Le projet vise le développement de nouveaux modèles mathématiques permettant des analyses prédictives dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Ces algorithmes, auto-apprenants, doivent permettre d'identifier, très tôt, des comportements à risque.

« Le réel enjeu est de limiter le recours aux réseaux financiers à des fins terroristes et, pour ce faire, de mieux détecter des mouvements considérés comme à risque. »

Au regard des événements dramatiques qui ont secoué la capitale française dans le courant du mois de novembre, les institutions financières vont sans aucun doute voir leurs exigences en matière de lutte contre le financement du terrorisme renforcées.

« Lutter contre le terrorisme exige de s'attaquer à son financement. En outre, une meilleure analyse des flux, des transactions et des comportements des clients doit permettre de mieux identifier les risques », explique Olivier Merlan, ex-spécialiste d'Europol et directeur général adjoint de Logos IT Services, société éditrice du logiciel iDETECT**.**

Ce logiciel, remarqué par Gartner, soutient les acteurs issus de la finance mais aussi du renseignement dans la réponse à apporter vis-à-vis de ces enjeux. Il permet une analyse efficiente des données, tant des transactions réalisées par les clients que des informations non-structurées, en vue de détecter les comportements anormaux, à risque.

« Le système financier est, forcément, utilisé par les groupements terroristes »

Comme d'autres, ils doivent vendre, acheter, réaliser des transferts de fonds. Tout ne peut pas passer par des systèmes informels ou des réseaux de confiance de paiement tels les hawalas. Ils ont aussi recours aux réseaux financiers formels qui, aujourd'hui, laissent encore passer beaucoup de choses. Le réel enjeu est de limiter le recours à ces réseaux à des fins terroristes, de mieux détecter des mouvements considérer comme à risque. »

Des comportements passés au crible

Si les exigences en matière de lutte contre le financement du terrorisme se renforcent, notamment à travers la quatrième directive européenne anti-blanchiment et son application effective au sein des divers États concernés, les « méchants » eux aussi s'adaptent.

« Il n'est pas compliqué, pour les groupements terroristes, d'utiliser des hommes de paille pour ouvrir un compte et effectuer des transactions, précise Olivier Merlan. Si les acteurs

financiers doivent tenter de découvrir les bénéficiaires ultimes pour des investissements, ce n'est pas forcément évident pour des opérations courantes. Bien sûr, il existe des listes de sanctions, sur lesquelles les noms d'individus dangereux figurent. Ces gens, toutefois, ne sont pas bêtes au point de s'exposer directement en utilisant leur propre nom. Pourtant, il y a un enjeu à pouvoir mieux analyser l'ensemble des transactions, afin de détecter des mouvements servant les intérêts de ces groupements. »

iDETECT, dès l'onboarding de clients et tout au long de la relation qu'ils entretiennent avec les services bancaires, permet de détecter des conduites à risque. Leur comportement sera passé au crible, aussi bien leurs transactions que ce qui est dit d'eux sur le web. Une analyse fine de données structurées et non- structurées peut révéler beaucoup de choses sur les intentions d'un client ainsi que sur l'environnement dans lequel il évolue. « Si le client n'est pas connu, on peut se rendre compte, en crawlant le web, que son nom peut résonner avec un environnement suspect. Le comportement d'un client peut évoluer, changer. Il est donc essentiel de l'analyser en continu », poursuit Olivier Merlan.

Détecter les facteurs à risque

Si iDETECT intègre déjà des modèles complexes permettant des analyses poussées, l'enjeu est d'aller un peu loin. Logos IT Services, avec l'un de ses clients basé au Moyen-Orient, entame un projet de recherche avec l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg pour développer de nouveaux modèles prédictifs. Ils doivent permettre de détecter des comportements à risque, bien en amont.

« À partir d'un environnement de données riche, allant bien au-delà de l'information transactionnelle, une analyse fine selon les modèles établis, il doit être possible de prévenir des problèmes bien avant qu'ils n'interviennent effectivement, poursuit Olivier Merlan. Il faut pouvoir modéliser les facteurs desquels peuvent découler un comportement à risque. » Certes, face à une large population, une quantité de données considérable, l'enjeu n'est pas évident.

Le Dr. Habil. Radu State du SnT ajoute : « Le sujet de recherche est très intéressant pour nous. Il établit une collaboration avec un partenaire industriel actif dans ce domaine et devrait, à ce titre, avoir un réel impact économique sur une thématique très actuelle et importante. Pour mener à bien ce projet, nous avons notamment beaucoup de verrous technologiques à lever. Ils portent sur l'analyse de grandes quantités de données (Big Data) ayant des structures sous-jacents complexes en termes de paramètres temporels et de types d'interactions. Sur le plan conceptuel, les défis fondamentaux portent sur les algorithmes à utiliser, leurs performances et leurs capacités d'apprentissage autonome par rapport à des contextes différents (cas par cas) d'usage. »

Ces mêmes techniques d'analyse ne s'appliquent pas qu'aux données financières. Pour toute population de données, il est possible de déterminer des comportements déviants –celui qui roule ou communique essentiellement la nuit, qui s'approche régulièrement des frontières ou d'aéroports, qui change régulièrement de téléphone, ou dont le rythme des revenus ou des dépenses varient de manière inhabituelle. C'est ensuite la combinaison fine de ces différents éléments en temps réel qui permet de déterminer ce qui s'écarte de la norme, de trouver l'aiguille dans la botte de foin et somme toute de stopper l'occurrence du comportement criminel avant que ce dernier ne puisse prendre place.

« Il faut donc s'appuyer sur le bon jeu de données. Les nouveaux modèles, surtout, au-delà de leur caractère prédictif, devraient être capables d'un niveau d'auto-apprentissage élevé même face à des comportements complexes et évolutifs, poursuit Olivier Merlan. Leurs analyses, dès lors, devraient s'affiner avec le temps, selon l'historique des informations dont ils disposent. »

Limiter les moyens d'actions des groupements terroristes

« L'enjeu est de limiter les moyens d'actions des terroristes et, pour cela, de pouvoir les anticiper. »

À terme, la lutte contre le financement du terrorisme devrait gagner en efficacité. « Nous sommes avant tout un fournisseur de technologie qui peut être mise au service de cette lutte contre le financement du terrorisme, poursuit le directeur adjoint de Logos IT Services. Le système, qui envoie des signaux d'alerte aux décideurs, est un outil clé. L'enjeu qui se cache derrière est de pouvoir couper les flux financiers qui profitent aux organisations terroristes. S'il devient plus difficile, pour eux, de louer un appartement ou une voiture, de manger, de financer d'autres achats, cela deviendra plus compliqué pour eux d'agir en toute impunité. L'enjeu est de limiter leurs moyens d'actions et, pour cela, de pouvoir les anticiper. »
http://www.itnation.lu/la-technologie-au-service-de-la-lutte-contre-le-financement-du-terrorisme/

Telegram,
Un outil de discussion prisé des djihadistes… mais pas seulement

Régulièrement décrite comme « l'application préférée des djihadistes », cette messagerie ne se résume pas à cela.
Les deux tueurs de Saint-Etienne-du-Rouvray (Seine-Maritime) l'utilisaient : Abdel-Malik Nabil Petitjean y a diffusé sa vidéo d'allégeance à l'organisation Etat islamique ; Adel Kermiche y a fait paraître, pendant plusieurs semaines, des messages annonçant qu'il allait faire *« un gros truc »*. Telegram, une application de messagerie populaire, est régulièrement décrite comme *« l'application préférée des djihadistes »*, mais ne se résume pas à cela.

C'est quoi ?

Telegram est une application de messagerie principalement utilisée sur téléphone portable, qui dispose de nombreuses fonctionnalités. Elle peut servir à la fois à communiquer directement avec une personne, y compris dans des « tchats secrets », chiffrés, ou à participer à des groupes de discussion. Elle permet également de partager facilement des photos et des vidéos.
Les principales fonctionnalités de l'application rappellent ses concurrents WhatsApp ou Facebook Messenger. Principale différence, Telegram propose aussi des « chaînes » publiques que les utilisateurs peuvent suivre, et l'application affirme qu'elle est particulièrement sécurisée et confidentielle.

Comment fonctionnent les « chaînes » de Telegram ?

On a beaucoup parlé de cette fonctionnalité après l'attentat de Saint-Etienne-du-Rouvray : l'un des auteurs de l'attaque animait l'une de ces chaînes, sur laquelle il avait annoncé préparer une action aux quelque 200 personnes qui le suivaient.
Les chaînes fonctionnent comme une messagerie à sens unique : seule la personne qui l'a créée, ou les personnes à qui il donne l'autorisation de publier des messages (des « administrateurs », dans le jargon de l'application), peuvent écrire des messages et y diffuser photos ou vidéos. Tout utilisateur peut a priori s'abonner à la chaîne, mais pour la trouver, il faut en connaître le nom – ce qui donne souvent aux utilisateurs l'impression que ces chaînes sont confidentielles.

Qui utilise Telegram ?

L'application revendique 100 millions d'utilisateurs dans le monde. Parmi eux, on compte certes des djihadistes – l'EI recommande d'utiliser cette application – mais aussi beaucoup d'autres personnes… Dont une bonne partie de la classe politique française.
En Iran, le service s'est imposé comme l'un des principaux canaux d'information : les Iraniens l'utilisent à la fois pour discuter et pour s'informer sur l'actualité, en s'abonnant à des « chaînes » qui ne sont pas censurées comme le sont Facebook ou Twitter.
http://www.lemonde.fr/pixels/article/2016/07/29/telegram-un-outil-de-discussion-prise-des-djihadistes-mais-pas-seulement_4976364_4408996.html

L'application de messagerie Telegram fait le ménage dans les comptes de l'État islamique

Ce service, qui permet de communiquer de manière sécurisée, voit s'échanger plus de 12 milliards de messages par jour. Son PDG estime que le gouvernement français est «aussi responsable» des attentats du 13 novembre que l'État islamique.

Baptisée «l'application favorite des djihadistes» par la presse américaine, Telegram a enfin décidé de réagir. Le service, sorte d'hybride entre le réseau social et la messagerie ultra-sécurisée, a annoncé mercredi soir avoir supprimé 78 comptes appartenant à des sympathisants de l'Etat islamique. L'entreprise va par ailleurs mettre en place des outils pour mieux signaler les «contenus répréhensibles». «Nous avons été très perturbés d'apprendre que les chaînes publiques de Telegram étaient utilisées à des fins de propagande djihadiste», a-t-elle expliqué dans un communiqué

Dans les faits, Telegram était informé de la présence djihadiste sur son service depuis longtemps. L'application est appréciée par les partisans de l'Etat islamique car elle permet une communication chiffrée, c'est-à-dire illisible en cas d'interception par les autorités, et peut même détruire les messages dès qu'ils sont lus. Telegram a été cité à plusieurs reprises dans les communiqués officiels de l'Etat islamique comme étant l'une des meilleures applications pour échanger des informations et diffuser de la propagande. C'est par ce biais que l'organisation terroriste a revendiqué les attentats du 13 novembre. Mercredi soir, certaines chaînes djihadistes supprimées tentaient déjà de revenir sur le service, d'après *Le Monde.* Une stratégie similaire est menée sur Twitter, également fréquentée par les partisans de l'Etat islamique, où certains comptes ont déjà été supprimés plus de 300 fois.

«C'est comme si on interdisait les mots parce qu'ils savent parler!»

Interrogé au sujet de la propagande djihadiste en septembre, Pavel Durov, cofondateur de l'application, avait expliqué que «le droit à la vie privée était plus important que notre crainte de subir de mauvaises choses, comme le terrorisme.» Il y a quelques jours, il avait réitéré ces propos. «Interdire Telegram parce que des terroristes l'utilisent, c'est comme si on interdisait les mots parce qu'ils savent parler!» a assuré Pavel Durov devant une proposition d'un parlementaire russe d'interdire son application. Ce discours a depuis sensiblement changé.

Pavel Durov s'est même fendu d'une autre déclaration sur son compte Instagram, où il accuse le gouvernement français d'être «aussi responsable que l'Etat islamique» des attentats du 13 novembre.

Avant d'avoir créé Telegram, Pavel Durov était le PDG de VKontkate, le premier réseau social russe. Il a néanmoins été forcé de s'exiler aux États-Unis après avoir perdu le contrôle de son entreprise. Il affirme avoir créé Telegram avec son frère afin d'échapper à la surveillance du gouvernement russe. L'application est d'ailleurs recommandée par Edward Snowden, fervent militant des libertés en ligne et à l'origine du scandale de la NSA. Telegram voit chaque jour s'échanger plus de 12 milliards de messages, soit 12 fois plus qu'en février.

http://www.lefigaro.fr/secteur/high-tech/2015/11/19/32001-20151119ARTFIG00069-l-application-de-messagerie-telegram-censure-78-comptes-de-l-etat-islamique.php

Attentats à Paris : Comment les terroristes ont-ils financé leurs attaques ?

Le Centre d'analyse du terrorisme a publié son rapport sur le financement des attentats perpétrés à Paris et Saint-Denis en janvier et novembre 2015.

Presque un an après l'horreur qui a traversé la capitale le vendredi 13 novembre 2015, un rapport nous apprend comment les responsables de la plus importante tuerie depuis la

Seconde Guerre mondiale sur le sol français l'ont financée. Le Centre d'analyse du terrorisme (CAT) a publié un rapport sur le financement des attentats perpétrés en Île-de-France en janvier et novembre 2015.

Un document qui revient à la fois sur le budget des terroristes, comment ils ont acquis l'argent et quelle somme a servi à quoi. Il détaille également des résolutions recommandées pour modifier certaines lois et mieux combattre de futures attaques. Le document pointe notamment l'anonymat garanti dans de nombreuses situations et qui ne permettrait pas de mener une véritable politique efficace en matière de lutte contre le terrorisme.

108.000 euros de budget total pour les attentats de janvier et novembre

D'après *Le Financement des attentats de Paris*, les attentats de *Charlie Hebdo* et de L'Hyper Cacher de Vincennes ont coûté 26.000 euros à leurs auteurs**, contre** 82.000 euros pour ceux du 13 novembre**.** Le rapport détaille ce à quoi a servi tout cet argent. Ainsi, il se divise pour chacun des actes meurtriers en six différentes utilités : « l'armement, les logements conspiratifs, les véhicules, les faux-papiers et les déplacements«.

Dans le détail, on apprend par exemple que le coût de l'armement des terroristes du 13 novembre est inférieur à celui utilisé en janvier par Amédy Coulibaly et les frères Kouachi.

Le premier avait un arsenal d'une valeur de 10.000 euros pour lui seul, quand les assassins des journalistes de*Charlie Hebdo* avaient des armes d'une valeur de 9.400 euros. Les membres du commando des terrasses et du Bataclan fin 2015 disposaient eux d'un armement d'une valeur totale de 16.000 euros, alors qu'ils étaient bien plus nombreux. Le document n'indique pas les raisons d'une telle différence, si ce n'est la provenance étrangère des AK-K7.

En revanche, la logistique des attentats à Paris et Saint-Denis ont requis des sommes importantes. 20.000 euros environ pour les différents logements, 11.000 pour les onze véhicules utilisés, 3.000 euros en téléphonie, 5.000 euros de faux papiers et 27.000 euros pour les déplacements (notamment les départs de Syrie vers l'Europe).

Diverses méthodes de financements

Dans ce rapport du CAT, les différents tuyaux de financements des attentats sont exposés. Des manières très différentes entre janvier et novembre. En janvier, les terroristes se sont auto-financés, tandis que ceux de novembre ont profité d'un réel soutien monétaire de l'Organisation État Islamique (OEI), qui a revendiqué les attentats. Pour les premiers donc, ils ont mis en oeuvre plusieurs techniques afin de réunir un budget suffisamment conséquent.

Selon le Centre d'analyse du terrorisme, Amédy Coulibaly et les frères Kouachi ont mis en place des systèmes de fraudes au crédit à la consommation (jusqu'à 34.000 euros pour le preneur d'otages de l'Hyper Cacher), mais aussi du commerce illicite, de vêtements de marque pour les frères Kouachi ou encore des **«** fonds propres **»**.

En revanche, pour les commandos de novembre, dont les attaques ont été préparées depuis la Syrie, l'OEI a largement participé de sa poche. « Ces montants varient entre 2.000 à 3.000 euros par personne«, précise le document. Cet argent serait distribué sous forme d'espèces au départ de Syrie ou via des transferts de fonds.

Le problème de l'anonymat pointé à plusieurs niveaux

Le CAT pointe ainsi de multiples failles dans notre système qui permettent aux terroristes de préparer de manière quasi sereine leurs ambitions funestes. À commencer par l'anonymat dans l'achat de cartes bleues prépayées**,** et le fait « qu'aucun document attestant de identité n'est demandé ». Des CB activés de plus anonymement par SMS. Des SMS envoyés et reçus sur un téléphone avec une SIM prépayée. C'est justement l'une des directives qui ressort d'un des numéros du magazine officiel de l'organisation terroriste basée en Syrie et en Irak, citée dans le rapport : « Vous devez impérativement avoir des téléphones achetés par exemple au bureau de tabac, débloqués, vous pouvez aussi avoir des cartes SIM dans n'importe quel taxiphone, et ensuite activer les cartes en question avec des fausses informations **».**

Autres soucis : les applications qui permettent aux terroristes en devenir d'échanger entre eux sans aucun contrôle. Ce n'est pas la première fois que des outils comme Telegram sont d'ailleurs pointés du doigt. Ils permettent en effet une protection totale à leurs utilisateurs.
« L'application Telegram a permis aux membres non-européens du commando du 13 novembre de rester en contact avec leur commanditaire Abou Ahmad », illustre le rapport.
À ces lacunes sécuritaires, le rapport répond en donnant de nombreuses pistes pour les combler. Notamment le fait de « s'inspirer de la Belgique et de l'Allemagne » sur l'interdiction de « l'anonymat pour l'achat des cartes SIM ». Car, comme dit le rapport, « les mesures prises dans un État (…) n'auront peu d'effet si elles ne sont pas adoptées par l'ensemble des autres État ». Et de prôner **«** une véritable politique d'échange d'informations entre les services de renseignement ».
http://cat-int.org/index.php/2016/10/20/attentats-a-paris-comment-les-terroristes-ont-ils-finance-leurs-attaques/