COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 25 avril 2016 CODEXTER (2016) 2

COMITÉ D'EXPERTS SUR LE TERRORISME

(CODEXTER)

TERRORISME ET INTERNET

DOCUMENT DE RÉFLEXION

30e Réunion plénière

Strasbourg (France), 19 – 20 novembre 2016

Secrétariat de la Division de la lutte contre le terrorisme
Direction de la société de l'information et de la lutte contre la criminalité, DG I

codexter@coe.int - www.coe.int/terrorism

Résumé

Le présent document de réflexion propose une vue d'ensemble des principaux défis découlant de l'utilisation d'internet à des fins terroristes. Quatre grands thèmes seront évoqués : les problèmes liés au cryptage des outils et des données ; le blocage et la suppression de sites web et de comptes de médias sociaux utilisés à des fins terroristes ; les questions de compétence liées aux données stockées dans d'autres juridictions, y compris sur le « nuage » ; l'identification des personnes physiques/morales qui se cachent derrière les adresses IP utilisées à des fins terroristes. Le document renvoie aux conventions et aux décisions judiciaires internationales et européennes pertinentes ainsi qu'à des études universitaires et à des articles en ligne de spécialistes du droit public. Enfin, le document propose une série de recommandations adressées au CODEXTER concernant d'éventuelles mesures à prendre au niveau international, et notamment la faisabilité d'une plateforme d'échange avec les grandes entreprises d'internet, qui serait établie dans le cadre de la Stratégie du Conseil de l'Europe sur la gouvernance d'internet (2016 – 2019).

1. Informations générales

Le 19 mai 2015, le Comité des Ministres a adopté le Plan d'action sur « la lutte contre l'extrémisme violent et la radicalisation conduisant au terrorisme » en vue de renforcer le cadre juridique relatif au terrorisme et à l'extrémisme violent et de prévenir et combattre la radicalisation violente au moyen de mesures concrètes dans le secteur public, en particulier les écoles et les prisons, et sur internet.

Observant qu'internet et les médias sociaux sont massivement utilisés par les personnes qui cherchent à recruter des combattants terroristes, le Comité des Ministres a pris conscience de la nécessité d'intensifier l'action dans ce domaine, dans le plein respect du principe fondamental de la liberté d'expression et d'information, tels qu'il est inscrit dans la Convention européenne des droits de l'homme.

Sur la base de son Mandat pour 2016 – 2017, le CODEXTER, lors de sa 29e réunion plénière, a examiné un document contenant des propositions de domaines prioritaires pour ses activités au cours du biennium et décidé de faire du terrorisme et d'internet la première priorité qu'il examinerait. Le CODEXTER a noté que le Conseil de l'Europe, au moyen de ses divers comités compétents, occupe une position unique pour faciliter la coopération internationale et prévenir l'utilisation d'internet par des terroristes pour propager leur message de haine et de terreur.

Lors de sa 7e réunion (16-17 mars 2016), le Bureau du CODEXTER a décidé de nommer M. Mario JANECEK (Bosnie-Herzégovine) en tant que coordinateur pour le thème « Terrorisme et internet ».

Afin de faciliter les délibérations du CODEXTER, le Secrétariat, en concertation avec le coordinateur, a demandé à M. Eirik Trønnes Hansen, procureur au Service national norvégien de renseignements criminel (NCIS), en tant qu'expert des questions liées à la cybercriminalité, de préparer un document de réflexion sur les principaux défis découlant de l'utilisation d'internet à des fins terroristes et de recenser les principaux problèmes et – éventuellement – les solutions à leur apporter.

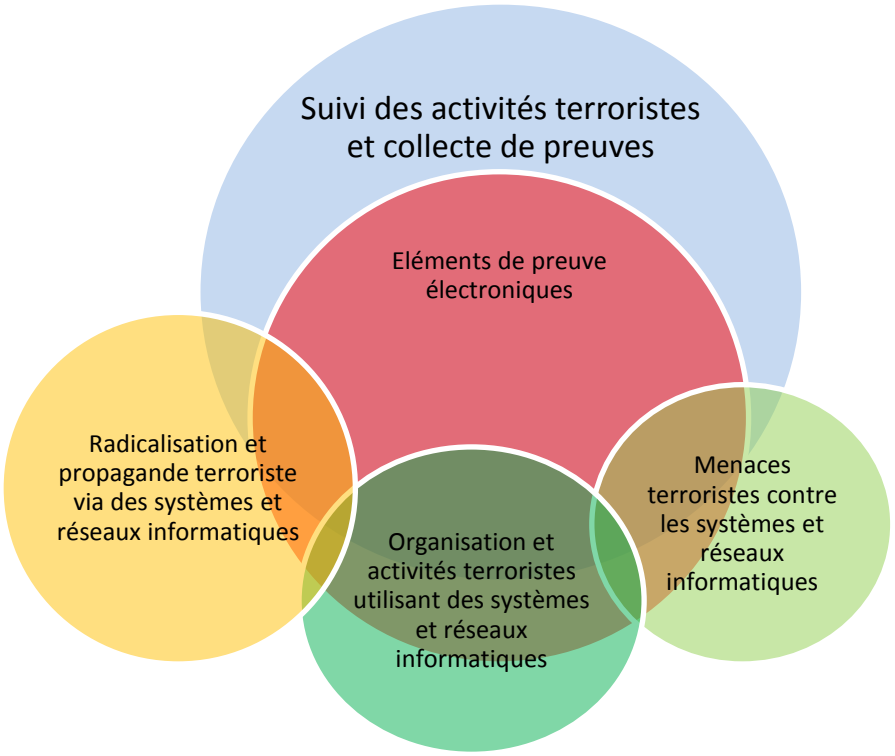
Le présent document est le résultat des travaux de M. Eirik Trønnes Hansen. Il vise à servir de base aux discussions du CODEXTER lors de sa 30e Réunion plénière. Ce document ne reflète pas nécessairement les positions du CODEXTER.

2. **Introduction**

Du fait de l'expansion constante d'internet – sa technologie, ses services et ses utilisateurs – son utilisation à des fins terroristes est de plus en plus un problème pour les forces de l'ordre et une menace pour la sécurité publique.

Dans le présent document, les définitions des termes « terrorisme » et « infraction terroriste » s'appuient sur l'article premier de la Convention du Conseil de l'Europe sur la prévention du terrorisme (STCE n° 196), selon lequel :
Aux fins de la présente Convention, on entend par « infraction terroriste » l'une quelconque des infractions entrant dans le champ d'application et telles que définies dans l'un des traités énumérés en annexe.

Cette annexe mentionne onze conventions internationales[i] : plusieurs de celles-ci concernent les actes terroristes contre les communications (aviation civile, navigation maritime), mais actuellement aucune convention ne porte spécifiquement sur le terrorisme contre les systèmes et réseaux informatiques ni sur l'utilisation de tels systèmes et réseaux à des fins terroristes. Ces questions peuvent cependant être couvertes par la Convention du Conseil de l'Europe sur la cybercriminalité (STCE n° 185). Dans sa Note d'orientation # 6 (4-5 juin 2013), le T-CY déclare que les attaques visant les infrastructures d'information critiques peuvent être couvertes par les articles 2, 3, 4, 5, 7, 8, 11 et 13 de la Convention. Ces articles s'appliqueraient aussi si une attaque pouvait être rattachée à des activités terroristes. Le T-CY travaille actuellement à une Note d'orientation sur le terrorisme et la Convention sur la cybercriminalité. De plus, les mesures énoncées dans la Convention pour la sécurisation des éléments de preuve électroniques s'appliquent aussi pour les affaires liées aux activités terroristes, y compris les articles 23, 25, 29 et 32. Les principaux problèmes actuels peuvent être représentés dans le schéma suivant :



Les éléments de preuve électroniques jouent souvent un rôle dans ces diverses activités, qui concernent à la fois les actes de terrorisme et l'action des forces de l'ordre contre le terrorisme. Un grand nombre de questions concernant les preuves électroniques et le terrorisme présentent des similitudes qu'il s'agisse d'activités terroristes ou d'autres types d'activités criminelles. Les terroristes utilisent très probablement les services internet à des fins de communication interne depuis que la technologie existe. Avec de plus en plus d'utilisateurs et de possibilités technologiques, même des mesures simples ont été utilisées par les terroristes pour réduire les risques de détection.

Le New York Times écrivait le 27 avril 2008 :

http://www.nytimes.com/2006/04/27/world/europe/27iht-spain.html?_r=0

« D'après le juge qui a instruit l'affaire, l'un des principaux inculpés pour les attentats à la bombe commis le 11 mars 2004 dans un train à Madrid a utilisé un procédé simple qui lui a permis de communiquer avec ses complices au moyen de comptes de messagerie électronique ordinaires sans être détecté par les autorités.

Au lieu d'envoyer les messages, le suspect, Hassan El Haski, les a sauvegardés en tant que brouillons sur des comptes qu'il partageait avec d'autres personnes radicalisées, d'après les documents communiqués par le juge, Juan del Olmo. Tous connaissaient le mot de passe et avaient donc accès aux comptes pour lire ses commentaires et poster des réponses.

Comme l'ont indiqué le juge et le gouvernement, grâce à ce subterfuge il n'y avait aucune trace numérique que les autorités auraient pu suivre aisément. Si le message électronique avait été envoyé, les autorités auraient pu le contrôler, ce qui est une pratique courante dans toute l'Europe.

Des responsables du renseignement avaient indiqué par le passé que les groupes terroristes utilisaient cette astuce, que certains enquêteurs appellent une « boîte aux lettres morte virtuelle », mais peu d'exemples concrets avaient été mis au jour, en particulier en lien avec un attentat aussi grave que les attaques de Madrid, qui ont fait 191 morts. »

Les expériences récentes concernant « l'Etat islamique/EIIL/Daech » ont accru l'intérêt du public et des forces de l'ordre pour la manière dont les terroristes utilisent internet et les autres systèmes et réseaux électroniques.

D'autres rapports ont été consacrés à des affaires spécifiques, par exemple le rapport de 2013 « Utilisation d'internet et des médias sociaux par Anders Behring Breivik » d'Aasland Ravndal, de l'Institut norvégien de recherches sur la défense (FFI), sur les attaques commises à Oslo et Utøya, en Norvège, le 22 juillet 2011 :

http://journals.sfu.ca/jed/index.php/jex/article/view/28
« Le présent article décrit l'utilisation d'internet et des médias sociaux par Breivik suivant quatre dimensions : (1) la radicalisation en ligne, (2) le jeu en ligne, (3) la préparation des attaques en ligne et (4) la propagande en ligne. (…)

Un résultat capital de cette étude est que Breivik n'a probablement jamais évoqué ses projets terroristes sur internet, avec qui que ce soit. De plus, ses commentaires sur divers forums internet ne se distinguent pas particulièrement des discours habituels d'extrême-droite en ligne.

En d'autres termes, les services de sécurité norvégiens ne réagiraient probablement pas aux messages qu'il a mis en ligne même s'il était sous surveillance. (…)

Les messages postés par Breivik indiquent aussi que ces vues critiques sur l'islam et le socialisme ***sont bien antérieures*** *à la création des blogs dits 'de lutte contre le djihad', ce qui signifie que ces blogs ont peut-être joué dans la radicalisation précoce de Breivik un rôle moins décisif que beaucoup l'ont supposé.*

Par la suite, cependant, ces blogs ont assurément renforcé la pensée radicale de Breivik, bien qu'ils paraissent bien moins radicaux que ses propres déclarations idéologiques après le 22 juillet. (…)

« La correspondance électronique de Breivik montre qu'il a avant tout voulu devenir ***auteur et éditeur*** *professionnel. Il a proposé de créer un 'journal sur papier conservateur et culturel avec des blogueurs norvégiens qu'il admirait, eux aussi critiques à l'égard de l'islam et du multiculturalisme. (…)*

*Le fait qu'****il ait été rejeté par plusieurs personnes qu'il estimait*** *peut avoir eu une influence décisive sur sa radicalisation. (…)*

Breivik ***a trouvé sur internet toutes les informations nécessaires pour fabriquer sa bombe****. Il a aussi* ***financé*** *les attaques terroristes au moyen d'une société en ligne et utilisé internet – en particulier eBay – pour acheter des matériels tels qu'un gilet pare-balles, des pièces d'armement et des composants pour fabriquer une bombe.*

Breivik a aussi fait un usage systématique de ***plates-formes de médias sociaux*** *telles que Facebook et Twitter à des fins de* ***propagande****. »*

Les attentats à la bombe de Madrid et les attentats d'Oslo et Utøya illustrent certaines limites pratiques : comment les forces de l'ordre peuvent-elles surveiller les messages électroniques lorsqu'aucun message n'est envoyé ? De plus, d'autres limites sont d'ordre juridique. Ainsi qu'il est indiqué dans le rapport de l'ONUDC, chapitre 1, B, I, n° 11 :

« Il est important de bien distinguer la simple propagande et les matériels destinés à inciter à commettre des actes terroristes. Dans plusieurs Etats membres, pour être reconnu coupable d'incitation au terrorisme, il faut que soient démontrée l'existence d'une intention et d'un lien de causalité directe entre la supposée propagande et le projet ou l'exécution effectifs d'un acte terroriste. Par exemple, dans une contribution aux réunions du groupe d'experts, un expert français a indiqué que la diffusion de documents instructifs sur les explosifs ne pouvait pas être considérée comme contraire au droit français sauf si la communication comportait des informations précisant que les documents étaient partagés à des fins terroristes. »

Ces limitations peuvent s'appuyer sur des droits protégés, tels que le droit à la liberté d'expression, le droit à la vie privée et le droit à la protection des données. Les solutions et les améliorations concernant la lutte contre le terrorisme doivent être contrebalancées avec ces principes et d'autres droits et garanties de la société civile. Plusieurs rapports et publications évoquent ces questions, parmi lesquels le rapport de l'ONUDC intitulé « L'utilisation d'internet à des fins terroristes » (2012).

https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Il existe des différences quant à la manière dont divers domaines des communications électroniques sont réglementés et celle dont les forces de l'ordre peuvent avoir accès aux données en question. Les entreprises traditionnelles de télécommunications qui proposent des services téléphoniques sont habituellement régies par des lois nationales spécifiques, qui prévoient souvent une obligation de confidentialité concernant les communications de leur clientèle, mais réglementent aussi la manière dont les forces de l'ordre peuvent avoir accès aux informations dans le cadre d'affaires pénales, notamment l'interception légale des communications. Les entreprises qui proposent divers services aux internautes le font généralement par-delà les frontières, ce qui complique les questions de juridiction. Ces entreprises et leurs données peuvent faire l'objet d'injonctions de produire, de perquisitions et de saisies, mais elles proposent parfois des services cryptés et/ou anonymisés, de sorte qu'il sera difficile ou impossible pour les forces de l'ordre d'avoir accès à des preuves électroniques utilisables.

Type	**Législation**	**Demandes directes de sa propre juridiction ?**	**Demandes directes d'autres juridictions ?**
Fournisseurs de services de	Dispositions nationales spécifiques	Certaines requêtes, selon la législation	Généralement non. Le droit interne l'interdit

télécommunication	sur les télécommunications, obligation de confidentialité.	nationale, par exemple des informations sur les abonnés.	parfois expressément.
Médias sociaux et services de courrier électronique (Google, MS, Facebook, VK…)	Lois sur la protection des données, accords d'utilisation, autres dispositions	Certaines requêtes, selon la législation nationale, par exemple des informations sur les abonnés. Injonction de produire ?	Certaines requêtes, selon la législation nationale, par exemple des informations sur les abonnés. Pratiques différentes aux Etats-Unis/ dans l'UE/ en Russie. Entraide judiciaire ?
Sociétés d'hébergement de sites web	Lois sur la protection des données, accords d'utilisation, autres dispositions	Certaines requêtes, selon la législation nationale, par exemple des informations sur les abonnés. Injonction de produire ?	Certaines requêtes, selon la législation nationale, par exemple des informations sur les abonnés. Pratiques différentes aux Etats-Unis/ dans l'UE. Entraide judiciaire ?
Autorités d'enregistrement	Lois sur la protection des données, accords d'utilisation, autres dispositions	Certaines requêtes, selon la législation nationale, par exemple des informations sur les abonnés. Injonction de produire ?	Dans une certaine mesure. Certaines données se trouvent sur des registres publics consultables. Entraide judiciaire ?

3. Problèmes liés au cryptage des outils et des données

3.1 Introduction

Le cryptage peut être décrit comme un processus par lequel l'information est modifiée de manière à ne pouvoir être lue que par les parties autorisées, par exemple l'expéditeur et le destinataire. Les systèmes de cryptage utilisent souvent deux clés : une clé publique, accessible à tous, et une clé privée, qui permet aux parties autorisées d'avoir accès aux informations en question. Certains dispositifs de cryptage sont proposés par les prestataires en tant que produits commerciaux, tandis que d'autres (par exemple OpenPGP) sont des normes ouvertes accessibles à tous.

Le cryptage peut être un outil précieux pour les utilisateurs individuels et les entreprises, leur permettant de protéger leur vie privée et de garantir des données contre l'intrusion et l'utilisation criminelle de données et de systèmes. Cependant, le cryptage peut rendre plus difficile, pour les

forces de l'ordre, l'accès à des données et des services qui auraient pu être utilisés pour recueillir des preuves dans des enquêtes criminelles, y compris dans des affaires de terrorisme.

Les difficultés juridiques et pratiques sont variables selon les situations, comme il est précisé ci-après.

3.2 Cryptage d'appareils non connectés détenus par le suspect

Pour les appareils non connectés détenus par le suspect, par exemple des disques durs, l'accès aux données cryptées peut poser problème d'un point de vue technologique, mais rarement sur le plan juridique. Dans certains cas, le mot de passe est connu. Il peut être écrit sur un morceau de papier retrouvé lors de la perquisition et saisie, ou stocké sur l'appareil. Parfois le suspect communique le mot de passe exact à la police. En Europe, les forces de l'ordre peuvent généralement utiliser le mot de passe pour déverrouiller l'appareil, du moins s'il a été obtenu légalement (perquisition et saisie, injonction de produire, etc.). Dans ces affaires, aucun intérêt de parties tierces n'entre en jeu.

Si le mot de passe exact n'est pas connu, les forces de l'ordre peuvent essayer d'utiliser des logiciels spécifiques ou d'autres méthodes pour le « deviner ». Cette pratique est généralement considérée comme une extension de la perquisition et saisie, et ne crée aucune question juridique nouvelle, du moins pour les appareils non connectés.

Certains Etats, comme le Royaume-Uni, ont des instruments juridiques qui peuvent obliger un suspect à révéler la clé de cryptage de données. Aux termes de la loi réglementant les pouvoirs d'investigation, article 49 (3),

« Une obligation de divulgation concernant une éventuelle information protégée est requise sur la base des motifs prévus par le présent paragraphe si elle est nécessaire :

(a) dans l'intérêt de la sécurité nationale ;

(b) à des fins de prévention ou de détection d'une activité criminelle ; ou

(c) dans l'intérêt du bien-être économique du Royaume-Uni. »

Cela inclut les enquêtes sur le terrorisme, y compris les activités des forces de l'ordre visant à prévenir les attentats terroristes.

D'après l'article 53 (5) (a) de cette loi, le non-respect d'une notification (« *s'il manque sciemment*… ») est passible de jusqu'à cinq ans de prison dans une affaire touchant à la sécurité nationale.

Des instruments juridiques analogues ont été envisagés dans d'autres Etats européens, mais ils visaient principalement à contraindre des parties tierces à donner accès à des données. La question de la déposition contre soi-même (cf. l'article 6 de la Convention européenne des droits de l'homme et la pratique correspondante de la Cour) peut se poser dans les affaires où les suspects seraient obligés de donner aux forces de l'ordre un accès à des données.

3.3 Cryptage d'appareils non connectés détenus par d'autres personnes

Des témoins ou d'autres parties tierces détiennent parfois des appareils non connectés contenant des informations pouvant servir de preuve. Ces appareils peuvent faire l'objet de perquisitions-saisies ou d'injonctions de produire, mais si les données en question sont cryptées, existe-t-il une obligation d'aider à leur déverrouillage ? La réponse à cette question dépend de la législation locale. Par exemple, aux termes de l'article 199 a de la loi norvégienne sur la procédure pénale :

« *Lors d'une perquisition sur un système de traitement de données, la police peut exiger de toute personne s'occupant du système en question les informations nécessaires pour y avoir accès. Un manquement à l'obligation de fournir des informations, s'il est commis par d'autres personnes que l'accusé, est sanctionné en vertu de l'article 339, n° 1, du Code pénal.* »

Outre la question de la déposition contre soi-même, l'accès aux données cryptées peut aussi poser un problème juridique si l'appareil est détenu par une personne n'ayant pas d'obligation de témoigner (membre de la famille proche) ou par une personne physique ou morale ayant une obligation de confidentialité protégée par la loi (avocats, prêtres, personnels médicaux, etc.). Sauf si la loi prévoit une exception à l'obligation générale de confidentialité dans les affaires de terrorisme, selon la législation locale, il peut être difficile ou simplement impossible de contraindre des membres de ces groupes protégés à divulguer des informations aux forces de l'ordre.

3.4 Services de télécommunications

Les services de télécommunications traditionnels sont généralement réglementés par des lois nationales, y compris des dispositions pouvant exiger des entreprises de télécommunications qu'elles rendent possibles techniquement les interceptions légales. Du fait de ces réglementations, il est souvent plus difficile, voire impossible, pour les opérateurs de téléphonie européens de proposer des services de téléphonie ne permettant pas une surveillance par les forces de l'ordre locale prévue par la législation et une ordonnance judiciaire.

3.5 Services internet autres que de télécommunications

Tandis que les services de téléphonie en Europe sont réglementés par les législations locales, et qu'ils étaient proposés, par le passé, par un opérateur public unique, de nouveaux services tels que la messagerie électronique, l'hébergement de sites web, les médias sociaux, les sites de discussion, le VoIP, etc. ne sont pas couverts par la réglementation sur les télécommunications. A la différence des entreprises de télécommunications, qui proposent habituellement leurs services traditionnels dans un pays clairement défini, les nouveaux services internet sont parfois proposés par-delà les frontières et souvent à l'échelle mondiale. Outre le fait qu'ils ne sont pas régis par les mêmes réglementations, les services internet autres que de télécommunications posent aussi la question de leur portée territoriale précise.

La plupart des services internet proposent une forme de protection du mot de passe afin d'empêcher toute utilisation abusive. Certains proposent un cryptage automatique, par exemple pour les

messages électroniques. D'autres services, comme l'hébergement de sites web, peuvent stocker des données cryptées par l'utilisateur.

D'une manière générale, il n'existe pas dans ces différents cas de réglementation nationale ou internationale spécifique pour le cryptage. Les forces de l'ordre ont la possibilité de s'adresser au service en question pour demander l'accès aux données. Toutefois, si celles-ci sont cryptées, que ce soit par l'utilisateur ou l'entreprise en question, le prestataire ne sera pas nécessairement en mesure de décrypter les messages de son propre service.

Comme on l'a vu dans l'introduction, le cryptage de données peut être une bonne pratique pour de nombreux utilisateurs. Plusieurs violations à grand échelle de la sécurité des données auraient pu être évitées si ces données avaient été cryptées. La protection des informations des personnes et des entreprises répond à un besoin réel. Dans certains cas, les forces de l'ordre doivent cependant avoir accès aux données et le cryptage paraît poser un problème de plus en plus difficile. Une injonction de produire est parfois possible légalement, mais le déverrouillage de l'appareil crypté n'est pas possible techniquement.

Une différence possible entre le cryptage des appareils non connectés et le cryptage des services en ligne tient au fait que les prestataires de services *pourraient* appliquer certaines limites au cryptage, avec une possibilité d'accès aux données transmises via leurs services. Cela serait comparable aux possibilités d'interception légale que les entreprises de télécommunications traditionnelles proposent dans un cadre juridique spécifique. De nombreuses entreprises et organisations de défense des droits opposent à cette position le fait que ces « portes dérobées » ne sont pas sûres et peuvent être utilisées par d'autres parties. En outre, la possibilité de telles « portes dérobées » peut affecter la confiance des consommateurs à l'égard de leurs produits et services.

Certains services internet n'ont pas un propriétaire identifiable ou une personne morale à contacter pour obtenir une aide au décryptage. C'est le cas par exemple de protocoles en source ouverte comme XMPP, un protocole de messagerie en ligne aussi connu sous le nom de Jabber. Ces protocoles peuvent être utilisés par un certain nombre de parties qui seront elles-mêmes difficilement identifiables. Une autre question concerne la capacité de ces parties à décrypter leurs services si cela leur est demandé.

BBC News rapportait le 5 avril 2016 que le service populaire de messagerie en ligne WhatsApp avait introduit le cryptage de ses services :

www.bbc.com/news/technology-35969739

« Au moyen du cryptage de bout en bout (end-to-end), les messages sont brouillés à leur départ de l'appareil de l'expéditeur et ne peuvent être décryptés que par l'appareil du destinataire. Les messages sont donc illisibles en cas d'interception, par exemple par des criminels ou par les forces de l'ordre. WhatsApp, qui compte un milliard d'utilisateurs dans le monde, a indiqué que les transferts de fichiers et les appels vocaux seraient également cryptés.

L'entreprise, qui appartient à Facebook, a déclaré que la protection des communications privées était l'une de ses « convictions fondamentales ». (…)

Les utilisateurs ayant la dernière version de l'application ont été informés de la modification lors de l'envoi de messages ce mardi. Le paramètre est défini par défaut. (…)

Une autre application de messagerie incluant un cryptage de bout en bout est notamment Telegram, connue pour être utilisée par l'« Etat islamique » pour partager des informations. »

En théorie, les gouvernements pourraient introduire des lois qui inscriraient les services internet dans un cadre juridique comparable à celui qui régit les services de téléphonie traditionnels. En partie du fait du caractère transnational de nombreux services internet, cela n'a pas encore était fait en Europe. Faute d'une réglementation des services WhatsApp aux Etats-Unis, puisqu'il s'agit d'une entreprise américaine, il serait difficile voire impossible pour des pays européens de réglementer les services de cryptage proposés par WhatsApp. Il serait également difficile ou impossible d'essayer d'interdire aux services WhatsApp d'utiliser les réseaux internet européens.

3.6 Cryptage d'appareils connectés

Le cryptage d'appareils connectés tels que des Smartphones confronte les forces de l'ordre à de nombreuses difficultés identiques à celles que présente le cryptage des services en ligne. Un exemple récent a été l'affaire San Bernadino[ii], dans laquelle le FBI a tenté de contraindre Apple à aider au déverrouillage d'un iPhone utilisé par l'un des auteurs de l'attaque du 2 décembre 2015.

Apple s'est opposé à une décision judiciaire l'obligeant à fournir un nouveau logiciel pour permettre aux agents d'avoir accès à un téléphone. La demande était limitée à la désactivation du mécanisme qui verrouille l'appareil si un mot de passe incorrect est saisi plusieurs fois. Cette mesure pourrait permettre au FBI de « deviner » le mot de passe après un nombre de tentatives illimité. Finalement, le FBI a renoncé à son action judiciaire, une tierce entreprise ayant proposé un logiciel pouvant donner accès au téléphone en question. D'après plusieurs sources, la méthode d'accès utilisée dans cette affaire pourrait ne pas fonctionner à l'avenir, Apple ayant actualisé le logiciel des iPhones et amélioré la sécurité.

Cet exemple illustre une différence entre l'accès des forces de l'ordre à des données de télécommunications et leur accès à des données provenant d'appareils ou de services : les législations nationales obligent habituellement les entreprises de télécommunications à concevoir leurs systèmes de telle sorte que l'interception légale soit possible, tandis que l'accès des forces de l'ordre à des appareils et systèmes cryptés ou protégés dépend de possibilités techniques qui peuvent devenir inutilisables après de futures actualisations ou autres modifications des logiciels.

Le cryptage d'appareils connectés est dans une certaine mesure lié au cryptage des services internet. Des sociétés comme Apple ou Google proposent divers services sur leurs iPhones, iPads et Android. Les forces de l'ordre peuvent donc avoir accès à certains services dans la mesure où les téléphones utilisent des services de télécommunication traditionnels, tandis que le cryptage rend plus

difficile, et de plus en plus impossible, l'accès aux données stockées sur les appareils. A des degrés divers, l'accès aux services internet utilisés par les appareils est plus difficile que l'accès aux données de télécommunication, en raison en partie du cryptage des services, mais aussi parce que les questions de juridiction liées aux services en ligne font que l'accès aux données demande plus de temps aux forces de l'ordre.

4. Blocage et suppression de sites web et de comptes de médias sociaux utilisés à des fins terroristes

Les sites web, les médias sociaux et autres services internet peuvent être utilisés par les terroristes et les organisations terroristes à des fins de radicalisation, de propagande et de communication. Une difficulté pour les forces de l'ordre consiste à identifier ces voies de communication, comme on l'a vu dans l'introduction. Certaines de ces voies de communication sont situées sur des plates-formes cryptées du *deep web*. D'autres sont des services accessibles publiquement, comme Facebook, Twitter, les services d'hébergement, etc. L'« Etat islamique » a dans une certaine mesure utilisé l'application de messagerie cryptée de bout en bout Telegram pour sa communication interne et à des fins de propagande.

De nombreux pays ont des dispositions générales qui pourraient être utilisées pour certaines actions contre des contenus en ligne, par exemple pour saisir des domaines internet relevant de leur juridiction. Par exemple, dans leur rapport « Mesures pour bloquer, filtrer et supprimer des contenus en ligne illégaux : Pays-Bas » remis au Conseil de l'Europe, A.R. Lodder & K.E. Sandvliet (Dép. d'Etudes juridiques transnationales, Centre pour le droit & internet de la Vrije Universiteit d'Amsterdam) déclarent ce qui suit :

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732764

*« **Il n'y a pas de réglementation spécifique sur les questions de blocage, de filtrage et de suppression dans le droit néerlandais**. Cependant, il existe une vaste jurisprudence, basée en premier lieu sur l'exemption de responsabilité pour les prestataires de services de la société de l'information, telle qu'énoncée à l'article 96c, livre 6, du Code civil (portant application de la directive 2000/31/CE de l'UE sur le commerce électronique). (…). (…)*

*D'une manière générale, les contenus illégaux peuvent être supprimés, bloqués ou retirés **en vertu d'une ordonnance judiciaire**, laquelle – aux termes de l'article 196c(5), livre 6 (6:196c) CCN – ne prend pas nécessairement en considération les divers 'rôles' du prestataire de services internet, ce qui signifie que les FAI qui relèvent de la disposition applicable au simple transit doivent eux aussi respecter cette ordonnance. Il est à noter que l'hébergeur est le FAI auquel il est le plus souvent demandé de supprimer des contenus. (…)*

*Le Code de procédure pénale néerlandais (CPPN) comprend une section spécifique sur les **infractions terroristes**. Par exemple, son article 126zi indique qu'une suspicion n'est pas nécessaire et qu'une simple indication d'infraction terroriste suffit pour qu'un enquêteur demande à un FAI des renseignements sur le nom, l'adresse, le code postal et le*

domicile. Concernant le filtrage, le gouvernement a indiqué qu'il ne fonctionnait pas correctement. En effet, en matière de terrorisme les contenus illégaux ne sont pas aussi manifestes que par exemple la pédopornographie, ce qui entraîne une atteinte disproportionnée au droit à la liberté d'expression. »

Bloquer des contenus en ligne, en particulier ceux d'autres juridictions, pose divers problèmes juridiques.

Plusieurs pays en Europe ont envisagé de bloquer et/ou de supprimer les comptes internet utilisés à des fins terroristes. Par exemple, de récentes modifications à la législation française ont permis les ordonnances de suppression. Certains ont critiqué ce type d'instruments juridiques, comme portant potentiellement atteinte à la liberté d'expression. Citons par exemple une déclaration de la Représentante de l'OSCE pour la liberté des médias, en date du 30 mars 2015 :

www.osce.org/fom/14276
« La Représentante de l'OSCE pour la liberté des médias, Dunja Mijatović, a déclaré aujourd'hui que les décisions unilatérales du ministère français de l'Intérieur, sans contrôle juridictionnel, de bloquer cinq sites web supposés avoir provoqué ou promu le terrorisme représentent une grave menace pour la liberté d'expression et la liberté des médias.

'Bloquer des sites web sans contrôle juridictionnel peut menacer la liberté d'expression et la liberté des médias et crée un risque manifeste de censure des contenus en ligne de la part des instances politiques », a déclaré Mme Mijatović.

La Représentante a exhorté les autorités françaises à réexaminer les parties de la loi contre le terrorisme, adoptée en novembre de l'année dernière, permettant le blocage de sites web. (…)

La Représentante a aussi noté avec inquiétude les débats parlementaires que connaissent plusieurs Etats membres de l'OSCE au sujet de dispositions pouvant avoir un impact analogue sur la liberté d'expression. Il s'agit par exemple de nouvelles dispositions pénales approuvées en Espagne concernant l'accès aux contenus extrémistes ou leur diffusion, et de certaines dispositions antiterroristes contenues dans le projet de loi C-51 au Canada. »

Ces inquiétudes pourraient être atténuées si le blocage de sites web était possible avec un contrôle juridictionnel, par exemple au moyen d'ordonnance d'un tribunal, mais si la liberté d'expression était cependant un motif de recours contre le blocage de contenus.

Une autre difficulté est d'ordre pratique. Si le contenu est bloqué, sa source peut simplement aller vers un autre forum internet, un autre nom de domaine ou un compte différent sur le même réseau social. Ce « combat sans fin » se rencontre aussi en lien avec d'autres types de contenus en ligne, du partage non autorisé de contenus protégés à la diffusion illégale de matériels sur des abus sexuels contre des enfants.

Outre les instruments juridiques nationaux, de nombreux services internet considèrent que l'utilisation par des organisations terroristes, etc., est une violation des accords d'utilisation. Les ordonnances judiciaires ou les législations nationales ne sont peut-être pas nécessaires pour retirer des contenus contraires à ces accords. Le 5 février 2016, le New York Times écrivait :

www.nytimes.com/2016/02/06/technology/twitter-account-suspensions-terrorism.html?_r=0

[Twitter] a suspendu 125 000 comptes Twitter associés à l'extrémisme depuis mi-2015. C'est la première fois que le nombre de comptes suspendus est rendu public. Twitter a également indiqué que les équipes chargées d'examiner les signalements de comptes liés à l'extrémisme avaient été renforcées, afin d'accélérer le retrait de ces comptes. (…)

Les 125 000 suspensions pourraient inclure des utilisateurs qui ont continué de créer de nouveaux comptes après que d'autres ont été suspendus, ce qui d'après les experts est une pratique courante parmi les partisans de l'EIIL.

Dans un message posté vendredi sur un blog, Twitter a déclaré que les menaces de violences et la promotion du terrorisme étaient de longue date contraires à ses règles d'utilisation. Depuis près de trois ans, Twitter coopère étroitement avec des groupes qui essaient de contrer les tactiques extrémistes au moyen de messages positifs, a indiqué la société. Elle a déclaré avoir décidé d'elle-même d'intensifier son action contre les messages extrémistes. »

Un autre exemple de service ayant bloqué des contenus et des comptes sur la base de ses accords d'utilisation et politiques internes est Telegram, qui propose des services de discussion et de messagerie cryptés de bout en bout. Dans une interview donnée à CNN le 23 février 2016, le fondateur de Telegram Pavel Durov a déclaré que la société n'avait jamais divulgué des données, mais qu'elle avait supprimé certains contenus liés au terrorisme :

www.cnn.com/2016/02/23/europe/pavel-durov-telegram-encryption
« (…) Durov affirme que les 'solutions simplistes' suggérées par les services de renseignement, qui consistent à bloquer l'accès aux applications et à permettre l'incursion des autorités pour sécuriser les communications, ne constituent pas une réponse adéquate.

Si vous y regardez de plus près, vous voyez que ces solutions ne fonctionneraient pas et qu'en réalité elles aggraveraient encore la situation', affirme-t-il. 'Elles consistent essentiellement, pour les entreprises qui proposent des services de messagerie cryptée, à appliquer des solutions de type « porte dérobée ».' Le problème d'une telle approche, affirme Durov, c'est qu'on ne peut pas créer une technologie de messagerie qui serait sûre pour tous sauf les terroristes. « Elle ne peut pas être sûre contre les criminels et ouverte pour les autorités. Soit elle est sûre, soit elle ne l'est pas, a-t-il déclaré. » (…)

Durov affirme que plusieurs gouvernements – dont celui de la Grande-Bretagne – ont sollicité son aide par le passé, mais le cryptage signifie que lui-même n'a pas accès aux messages de ses utilisateurs.

En deux ans et demi d'existence, nous n'avons pas divulgué un seul octet de données de nos utilisateurs', se vante-t-il. (…) Telegram est intervenu pour fermer des canaux publics de son application utilisés par l'EIIL. Selon les derniers chiffres, la société indique en avoir fermés 600.

Chaque jour, quatre ou cinq canaux sont signalés par nos utilisateurs et nous les supprimons, explique Durov. »

Les pratiques de services comme Twitter et Telegram indiquent que le blocage de contenus fondé sur une violation de l'accord d'utilisation peut être plus facile à appliquer que le blocage fondé sur la législation nationale.

Toutes conclusions ou recommandations du CODEXTER devraient prendre en compte les recommandations antérieures du Conseil de l'Europe sur le même sujet. Le Comité directeur du Conseil de l'Europe sur les médias et la société de l'information a approuvé une Recommandation CM/Rec(2014)6 sur un Guide des droits de l'homme pour les utilisateurs d'internet. Cette recommandation a été adoptée par le Comité des Ministres le 16 avril 2014 lors de la 1197e réunion des Délégués des Ministres. Dans son Annexe, le filtrage et le blocage sont évoqués :

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000016804d5b31

« 49. Des mesures générales de blocage ou de filtrage ne devraient être prises par les pouvoirs publics que si le filtrage concerne un contenu spécifique et clairement identifiable, sur la base d'une décision au sujet de l'illégalité de ce contenu prise par une autorité nationale compétente et qui peut être réexaminée par un tribunal ou une entité de régulation indépendante et impartiale, en accord avec les dispositions de l'article 6 de la CEDH. (…)

51. Le filtrage et la désindexation de contenus internet par des moteurs de recherche comportent le risque de violer la liberté d'expression des utilisateurs. Les moteurs de recherche ont la liberté d'explorer et d'indexer les informations diffusées sur internet. Ils ne devraient pas être tenus d'exercer un contrôle proactif de leurs réseaux et services afin de déceler un éventuel contenu illicite et ne devraient pas non plus réaliser des activités préalables de filtrage ou de blocage sans qu'il leur soit ordonné de le faire par une ordonnance judiciaire ou par une autorité compétente. (…)

53. Il est possible que des sociétés, comme les réseaux sociaux, suppriment des contenus créés et mis à disposition par des utilisateurs d'internet. Ces sociétés peuvent aussi désactiver le compte d'utilisateurs (par exemple, le profil d'un utilisateur ou sa présence sur les réseaux sociaux) en justifiant leur décision par le non-respect des conditions générales d'utilisation de leurs services. De telles mesures peuvent constituer une ingérence dans le droit à la liberté d'expression et celle de recevoir ou de communiquer des informations, à moins que ne soient réunies les conditions prévues à l'article 10, paragraphe 2, telles qu'interprétées par la Cour européenne des droits de l'homme. (…)

55. Guide alerte les utilisateurs d'internet sur le fait que les fournisseurs de services en ligne qui hébergent des contenus créés par les utilisateurs peuvent exercer différents niveaux de contrôle éditorial sur le contenu de leurs services. Sans préjudice de leur indépendance éditoriale, ils devraient faire en sorte que le droit des utilisateurs d'internet de rechercher, de recevoir et de diffuser des informations ne soit pas bafoué, en vertu de l'article 10 de la CEDH. Cela signifie que toute restriction appliquée à des contenus générés par les utilisateurs devrait être spécifique, justifiée pour permettre la restriction et communiquée à l'utilisateur concerné. (…)

59. Le Comité des Ministres du Conseil de l'Europe a affirmé le principe de l'anonymat dans sa Déclaration sur la liberté de la communication sur l'internet. En conséquence, afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations, les Etats membres du Conseil de l'Europe devraient respecter la volonté des usagers d'internet de ne pas révéler leur identité. Toutefois, le respect de l'anonymat n'empêche pas les Etats membres de prendre des mesures pour retrouver la trace de ceux qui sont responsables d'actes délictueux, conformément à la législation nationale, à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et aux autres traités internationaux dans le domaine de la justice et de la police. »

Dans un rapport réalisé pour la Conférence des Ministres du Conseil de l'Europe responsables des médias et de la société de l'information, intitulé « Liberté d'expression et démocratie à l'âge numérique : opportunités, droits et responsabilités » (Belgrade 7-8 novembre 2013), le professeur Ian Brown, de l'Université d'Oxford, écrivait ce qui suit (page 22-23) :

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000001680485444

« Les politiques menées par les États pour assurer la sécurité nationale et lutter contre le terrorisme posent d'autres problèmes délicats pour la liberté d'expression, de réunion et d'association. Les principes de droit international résumés par Frank La Rue, Rapporteur spécial de l'ONU, offrent un bon point de départ à la réflexion. Il propose par exemple que l'interdiction de soutenir des activités et organisations terroristes ne soit appliquée que pour restreindre les propos qui appellent sciemment à des actes de violence imminents et sont susceptibles de les provoquer, et jamais aux débats politiques, aux élections, aux informations concernant les droits de l'homme, les actions des pouvoirs publics ou la corruption des agents publics, aux manifestations pacifiques/ activités politiques et à l'expression d'une opinion, d'un désaccord, d'une religion ou d'une croyance, y compris de la part de minorités et d'autres groupes vulnérables.

Le Comité des Ministres devrait envisager de recommander d'autres normes positives et procédurales concernant la protection contre les poursuites et les autres mécanismes d'autorégulation et de co-régulation (en s'appuyant sur ses recommandations relatives aux filtres, aux réseaux sociaux et aux moteurs de recherche), et d'élaborer des procédures juridiques permettant aux tribunaux d'ordonner un blocage en tenant pleinement compte de son impact sur la liberté d'expression, de réunion et d'association. Ces règles pourraient s'inspirer des normes de procédure dérivées par la Cour des articles 6 (droit à un procès équitable) et 13 (droit à un recours effectif) et des limites que la Cour a posées aux ingérences dans les droits garantis aux articles 8, 10 et 11, ingérences qui doivent :

- *reposer sur des règles juridiques claires, accessibles et prévisibles (et dans la mesure du possible inscrites dans la loi) ;*
- *répondre à un « besoin social impérieux » ;*
- *n'être ni inefficaces, ni disproportionnées par rapport à l'objectif ;*
- *prévoir un « recours effectif », de préférence judiciaire, si ces critères ne sont pas remplis. »*

Concernant le contrôle juridictionnel et les recours effectifs, il convient de tenir compte du fait qu'une part importante des contenus liés au terrorisme visés par les mesures de retrait peuvent provenir de parties non identifiées, relevant d'autres juridictions, et que leur volume peut être important. Comme on l'a vu, de mi-2015 à février 2016, Twitter a suspendu 125 000 comptes associés à l'extrémisme. Pour les services de médias sociaux, le blocage de contenus se fait pour un seul compte à la fois.

S'il devait y avoir un mécanisme juridique national concernant le blocage des contenus en ligne, notamment des sites web hébergés dans d'autres juridictions, un filtrage au niveau des FAI serait probablement nécessaire. Pour que ce type de filtrage de contenus soit efficace, chaque pays devrait probablement à la fois mettre en place un mécanisme juridique applicable à tous les FAI relevant de sa juridiction et s'assurer que la totalité – ou du moins une large majorité – des FAI disposent réellement d'un système technologique leur permettant de bloquer des sites web.

Pour ce qui concerne le « recours effectif » et la nécessité d'ordonnances judiciaires, il pourrait aussi être tenu compte du fait que la question n'a pas été soulevée au sujet des spam. Comme l'indiquait le rapport susmentionné de Lodder et Sandvliet, « *si les FAI ne filtraient pas les spam, plus personne probablement n'utiliserait les courriers électroniques* ». Seul un petit nombre des parties responsables de l'envoi de spam, voire aucune, ne porte plainte auprès des FAI ou des tribunaux locaux lorsque leur contenu est bloqué par les filtres anti-spam. Cependant, ce qu'une partie qualifiera d'activités terroristes en ligne pourra être considéré par d'autres comme des déclarations politiques, et celles-ci peuvent bénéficier d'un niveau de protection supérieur à celui des activités commerciales.

Un autre exemple, concernant le déréférencement des contenus, est la pratique actuelle de moteurs de recherche comme Google et Microsoft Bing, basée sur le principe du « droit à l'oubli ». S'appuyant sur une décision de 2014 de la Cour de justice de l'UE[iii], Google et Microsoft ont créé le site web https://Forget.me pour recevoir les demandes de retrait ou de déréférencement de contenus de Google et Bing. Les demandes sont traitées par Google ou Bing, non par une autorité publique quelconque, et leur procédure est apparemment non contradictoire.

Il existe actuellement un mécanisme de filtrage pour les matériels pédopornographiques, CIRCAMP[iv]. Quatorze pays européens font partie de ce réseau, cofinancé par le Programme pour un internet plus sûr de la Commission européenne. En théorie, une approche similaire pourrait être utilisée pour bloquer les contenus en ligne liés au terrorisme, mais cela devrait probablement être réalisé en tant qu'initiative distincte plutôt que comme une extension du programme actuel.

Le filtrage de contenus en ligne ne va pas sans certaines controverses. Un des arguments de ses détracteurs est qu'il ne fonctionne pas ; un autre est qu'un système de filtrage efficace serait comparable à ce qu'on appelle le « grand pare-feu de la Chine »[v]. Un filtrage de grande ampleur des contenus en ligne ne serait pas acceptable dans le cadre européen, du fait des restrictions éventuelles à la liberté d'expression et des questions de censure. D'un autre côté, un filtrage ou un blocage de contenu, plus ciblé et limité à certaines finalités, pourrait être acceptable, sur la base des principes et approches décrits précédemment.

Avant même la question du blocage ou du retrait de contenus, il convient de s'interroger sur le type de contenus auquel ces mesures s'appliqueraient, sur la manière dont les contenus sont publiés ou diffusés, sur le lieu où ils le sont, et aussi sur la faisabilité d'un tel blocage ou filtrage. Des situations différentes pourront nécessiter des solutions technologiques et juridiques elles aussi différentes. Voici quelques exemples de contenus indésirables retirés, bloqués, filtrés ou déréférencés sans aucune procédure contradictoire publique :

- les spam : marquage et/ou retrait par les FAI, les fournisseurs de services de courrier électronique et/ou les services comme Spamhaus.
- les violations de la vie privée : déréférencement par les moteurs de recherche, sur la base de plaintes.
- les contenus contraires aux accords d'utilisation : suspension de comptes, décidées par les entreprises des médias sociaux, les hébergeurs de sites web, etc.

D'un autre côté, il convient de veiller à ne pas trop étendre ces pratiques. La liberté d'expression, la liberté d'accès à l'information, le droit à une procédure équitable et la transparence publique sont des droits fondamentaux et des attentes essentielles de la part du public européen. Cela vaut aussi pour les matériels et contenus posant des difficultés ou des problèmes particuliers.

5. Questions de compétence liées aux données stockées dans d'autres juridictions, y compris sur le « nuage »

Les données informatiques stockées peuvent servir de preuves dans des enquêtes criminelles, y compris dans des affaires de terrorisme. Différents types de données peuvent présenter un intérêt en tant que preuve :

- les informations sur les abonnés ;
- les données relatives au trafic ;
- les données relatives au contenu.

Il existe aussi différents types de fournisseurs de services internet, parmi lesquels :

- les services de télécommunications ;
- les médias sociaux et les services de messagerie électronique (Facebook, Microsoft, Google, VK, etc.) ;
- les hébergeurs de sites web ;
- les autorités d'enregistrement ;
- les proxys, VPN et autres fournisseurs de services d'anonymat ;
- les fournisseurs de services financiers en ligne (PayPal, Western Union, TransferWise, etc.)

L'accès à ce type de données, surtout lorsqu'elles sont stockées et traitées par des services liés à internet, pose certaines questions concernant la compétence, et notamment :

- la nationalité/localisation de la victime ;
- la nationalité/localisation du suspect ;
- le siège de la société qui traite les données ;
- les autres locaux de la société qui traite les données, par exemple un bureau régional de contrôle des données ;
- la localisation physique du serveur sur lequel les données sont stockées ;
- les solutions à plusieurs niveaux.

Toutes ces options sont aujourd'hui utilisées par différents pays, différentes entreprises et différents secteurs juridiques. En matière d'accès des forces de l'ordre aux données dans les enquêtes

criminelles, y compris dans les affaires de terrorisme, la compétence peut être déterminée différemment selon le contexte.

Plusieurs grandes entreprises proposant des services en ligne sont basées aux Etats-Unis. Pour les forces de l'ordre de pays européens, il peut être à la fois plus facile et plus difficile d'avoir accès à des données provenant des Etats-Unis, par rapport à des données d'autres pays européens. De grandes entreprises comme Google, Facebook, Microsoft et Apple ont des équipes spécialement chargées de répondre aux demandes des forces de l'ordre et publient souvent des lignes directrices à leur usage. Celles-ci peuvent différer légèrement d'une entreprise à une autre. La solution peut aussi être différente pour les petites entreprises ou celles du secteur de l'hébergement.

- Les informations relatives aux abonnés sont souvent disponibles en réponse à des demandes directes à l'entreprise en question, sur la base du droit américain et des pratiques propres à l'entreprise
- Les informations relatives aux données (courrier électronique, historiques de conversations, photos et documents stockés, etc.) ne sont habituellement disponibles que sur demande d'entraide judiciaire, et après délivrance d'une ordonnance par une juridiction des Etats-Unis, mais les données en question peuvent être conservées temporairement après une demande directe (cf. l'article 29 de la Convention sur la cybercriminalité (Convention de Budapest)).

De nombreuses grandes entreprises d'internet publient des rapports de transparence, comprenant des descriptions et des statistiques sur les demandes des forces de l'ordre. Par exemple :

- Google : https://www.google.com/transparencyreport/
- Microsoft : https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/
- Facebook : https://govtrequests.facebook.com/

De nombreuses entreprises du domaine des télécommunications proposent elles aussi des rapports de transparence. Les données de télécommunications sont réglementées par d'autres dispositions que celles qui s'appliquent aux données des entreprises proposant des services internet. A la différence de celles-ci, les entreprises du domaine des télécommunications ne fournissent habituellement des données qu'aux forces de l'ordre de leur territoire, et ne peuvent pas fournir de données à des filiales ou entreprises apparentées d'autres juridictions. Des entreprises comme Vodafone et Deutsche Telekom ont publié des rapports de transparence pour leurs différentes filiales et entreprises apparentées, pays par pays.

- Vodafone : https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html
- Deutsche Telekom : https://www.telekom.com/dataprotection et https://www.telekom.com/transparency-report

Dans son rapport de 2014 (https://www.telekom.com/corporate-responsibility/data-protection/transparency-report/297130), Deutsche Telekom déclarait ce qui suit :

« Deutsche Telekom ne répond pas aux demandes d'autorités extérieures à l'Allemagne. Toute demande de cette nature doit être soumise à Deutsche Telekom par le biais de l'autorité allemande compétente. »

Bien que cela ne soit pas mentionné dans le rapport de 2015, il ne faut pas nécessairement y voir un changement de pratique.

L'Institut national des normes et de la technologie (NIST), aux Etats-Unis, a défini l'informatique en nuage comme « *un modèle permettant un accès en réseau à la demande, omniprésent et pratique, à un fonds commun de ressources informatiques configurables (par exemple des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être fournies et communiquées rapidement, au moyen d'un minimum d'activité de gestion ou d'interaction du fournisseur de services.* »

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Une des caractéristiques de base de l'informatique en nuage tient au fait que les données peuvent être stockées et récupérées en différents lieux. Dans la pratique, le stockage et l'accès peuvent se faire dans le monde entier, et les données peuvent être déplacées rapidement. Le plus souvent, l'utilisateur final ne sait pas où les données sont stockées.

Le Conseil de l'Europe (T-CY) travaille actuellement sur ces questions. Un groupe de travail, le Groupe sur les preuves dans le nuage, présentera un rapport final en novembre 2016. Un document de réflexion remis par ce groupe au Comité du CdE de la Convention sur la cybercriminalité le 26 mai 2015[vi] cite une difficulté pour les forces de l'ordre :

« Avec l'informatique dans le cloud, les données sont rarement contenues dans un périphérique spécifique ou dans des réseaux fermés mais réparties entre différents services, fournisseurs, lieux et, souvent, différentes compétences : »

Ce document renvoie ensuite au projet de rapport du NIST, « *Cloud Computing, Forensic Science Challenges* » (voir chapitre 4, Analyse préliminaire):

http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

« Dans le domaine de l'enquête informatique traditionnelle, du fait du caractère centralisé du système des technologies de l'information, les enquêteurs peuvent exercer un plein contrôle sur les objets d'enquête (routeur, historiques des processus, disques durs). Cependant, sur l'écosystème du nuage, du fait de la diffusion des systèmes des technologies de l'information, le contrôle sur les couches fonctionnelles varie selon les acteurs du nuage, en fonction du modèle des services. Pour les enquêteurs, la visibilité et le contrôle sur les objets d'enquête sont donc réduits. »

A ces difficultés technologiques s'ajoutent plusieurs difficultés pratiques et juridiques. Ces difficultés ne sont pas spécifiques à l'informatique en nuage, mais le caractère transfrontalier de celle-ci accroît les difficultés. L'une d'elle a trait au temps. L'accès aux données stockées dans d'autres pays dépend souvent de l'entraide judiciaire. Ces processus reposent sur des pratiques anciennes, utilisant souvent des documents sur papier adressés par courrier traditionnel par l'intermédiaire de plusieurs parties.

Malgré la Convention de Budapest et les divers instruments et initiatives de coopération européens, un certain temps s'écoule entre le moment où une demande est envoyée et celui où les données en question sont disponibles. Souvent, les données demandées ne sont qu'une partie d'un ensemble de preuves, et d'autres preuves pourront nécessiter de nouvelles demandes dans d'autres pays. Dans le document de réflexion du T-CY susmentionné, le Groupe sur les preuves dans le nuage déclarait ce qui suit :

« L'entraide judiciaire demeure le principal moyen d'obtenir des éléments de preuve auprès de juridictions étrangères à des fins de procédures pénales. En décembre 2014, le comité de la Convention Cybercriminalité (T-CY) a mené une évaluation du fonctionnement des dispositions concernant l'entraide judiciaire. Il a conclu notamment que :

'Le processus de demande d'entraide judiciaire (DEJ) est jugé inefficient en général, et en particulier pour ce qui concerne l'obtention de preuves électroniques. Il semble que les délais de réponse à une demande aillent de six à 24 mois. Bon nombre de demandes et donc d'enquêtes sont abandonnées. Ceci pénalise l'obligation positive des gouvernements de protéger la société et les personnes contre la cybercriminalité et d'autres crimes impliquant des preuves électroniques.'

Le comité a adopté une série de recommandations visant à rendre le processus plus efficient. Il convient de mettre en œuvre ces recommandations.

Il y a lieu d'ajouter cependant que, pour les raisons que l'on vient de citer, l'entraide judiciaire n'offre pas toujours une solution réaliste pour accéder aux éléments de preuves stockés dans le nuage. »

6. L'identification des personnes physiques/morales qui se cachent derrière les adresses IP utilisées à des fins terroristes

Un rapport du 3 décembre 2014 du T-CY du Conseil de l'Europe décrit dans son introduction l'importance des adresses IP dans les enquêtes criminelles (Section 1, page 4).

http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf

« L'obtention d'informations auprès de fournisseurs d'accès internet pour identifier l'utilisateur (abonné) d'une adresse spécifique de protocole internet (IP) à un moment précis ou, vice-versa, pour identifier les adresses IP utilisées par une personne déjà connue, est essentielle dans le cadre d'enquêtes et de procédures pénales en matière de cybercriminalité et de preuve électronique. Les données relatives aux abonnés sont également les données les plus souvent recherchées dans le contexte de la coopération internationale. (…) Les adresses IP peuvent être considérées comme des données relatives aux abonnés – par opposition à données relatives au trafic – si l'objectif est d'obtenir l'identification d'un abonné utilisant une adresse IP. »

Pour citer les conclusions (Section 3, page 31) :

« En conclusion :

- *La plupart des Parties font la différence entre « données relatives aux abonnés » et « données relatives au trafic » ;*
- *Dans certains pays, l'atteinte aux droits fondamentaux est considérée comme étant nettement différente selon qu'il s'agit de l'obtention de données relatives aux abonnés, y compris concernant une adresse IP, dans le cadre d'une enquête pénale spécifique d'une part, ou de données relatives au trafic d'autre part ;*
- *En conséquence, dans ces pays, des règles différentes devraient-elles s'appliquer pour l'obtention des informations en question ;*
- *Les conditions requises pour l'obtention des données relatives aux abonnés sont, à l'heure actuelle, relativement variées ;*
- *Néanmoins, une plus grande harmonisation des règles en matière d'obtention des informations relatives aux abonnés faciliterait la coopération internationale.*
- *Il est recommandé au T-CY :*
- *de favoriser une plus grande harmonisation entre les Parties concernant les conditions, les règles et les procédures en matière d'obtention des données relatives aux abonnés ;*
- *d'encourager les Parties à tenir compte des observations du présent rapport lors de la refonte de leur législation interne. »*

Les divers pays et juridictions présentent des différences concernant les dispositions légales et réglementaires relatives à l'accès légal aux informations sur les abonnés. Du fait de ces différences, il peut être plus difficile et plus long d'identifier le client qui se cache derrière une adresse IP.

Un autre problème tient au fait que selon les entreprises et les secteurs technologiques, les pratiques varient en matière de stockage des informations sur les abonnés et des historiques des utilisateurs : par exemple les informations requises pour ouvrir un compte auprès d'un prestataire de services, le partage d'informations entre les entreprises et leurs partenaires, revendeurs, etc.

- Fournisseurs de services de télécommunication : souvent une réglementation nationale, par exemple pour exiger l'exactitude et l'exhaustivité des informations sur l'utilisateur, l'adresse physique, les informations de paiement, etc. ;
- Médias sociaux et fournisseurs de messagerie électronique : le plus souvent non réglementés ;
- Autorités d'enregistrement : le plus souvent non réglementées ;
- Services de cryptage et de préservation de l'anonymat : le plus souvent non réglementés.

Il existe toutefois une réglementation pour toutes les instances qui traitent des données à caractère personnel : la réglementation sur la protection des données. Un exemple est la directive 95/46/CE de l'UE relative à la protection des données. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.ENG

Aux termes de son article 6 (c), les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ». Ce principe peut aussi s'appliquer aux informations sur les abonnées et aux logs d'IP. L'Autorité norvégienne de protection des données a décidé en 2009 que deux fournisseurs de services internet devaient supprimer les logs d'IP de leurs clients après 21 jours, du fait que le stockage ou l'utilisation ultérieurs de cet ensemble de données n'étaient pas nécessaires à des fins de facturation ni à d'autres fins pour lesquelles les données avaient été collectées.
La conservation de données est un moyen de conserver des informations permettant de « revenir en arrière » et d'essayer d'associer des logs d'IP à des utilisateurs identifiés. Une décision du 8 avril 2014 de la Cour de justice de l'UE a invalidé la directive de l'UE sur la conservation des données.
http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Après cette décision, divers pays de l'UE ont adopté différentes solutions. Certains ont mis en œuvre des lois nationales sur la conservation des données ; d'autres ne prévoient aucune conservation des données. Cette situation rend plus difficile, pour les forces de l'ordre, le traçage des données jusqu'à un utilisateur final identifiable.

Avec les réseaux de communication sans fil et autres réseaux partagés, une adresse IP peut être partagée par de nombreux utilisateurs. Avec les services d'intermédiation (proxy) et de préservation de l'anonymat, il est devenu plus difficile, voire impossible, de remonter d'une adresse IP jusqu'à l'utilisateur. Au mieux, l'identification requiert une ou plusieurs étapes supplémentaires par le biais de divers fournisseurs. Un exemple simple à ce sujet est le suivant :
http://people.opera.com/howcome/2009/unlikely-places/
« En janvier [2009], l'Autorité de Chicago en charge du transit a remarqué que de nombreux internautes norvégiens suivaient la circulation des bus de Chicago en ligne. (…) Ces 'Norvégiens' étaient plus probablement des utilisateurs d'Opera Mini qui se trouvaient utiliser les parcs de serveurs d'Opera situés à Oslo. Les octets se trouvent un chemin en passant par des endroits improbables. »

Une autre difficulté est la migration vers de nouvelles technologies d'internet. D'après l'Etude d'Europol sur la menace du crime organisé sur internet (IOCTA) 2014 :
https://www.europol.europa.eu/iocta/2014/chap-4-3-view1.html
« Le nombre des adresses IPv4 diminue rapidement. La migration vers le protocole IPv6 – qui permet un nombre quasiment illimité d'adresses IP – avance mais sa mise en œuvre prendra probablement un temps considérable, ce qui signifie que pendant la période de transition, qui pourrait durer plusieurs années ou plus, d'autres manières d'assigner les adresses IP sont appliquées par les opérateurs afin de garantir la continuité du trafic internet dans un marché en expansion. La solution intermédiaire appelée Carrier-grade NAT (CGNAT) est maintenant utilisée par les opérateurs de services internet de l'UE.
La possibilité d'associer les utilisateurs à une adresse IP est cruciale dans les enquêtes criminelles. Lorsque le CGNAT est utilisé, de multiples appareils sont connectés sur un réseau local n'ayant qu'une adresse IP unique. ***Cette technologie permet potentiellement aux fournisseurs de connecter des milliers***

d'utilisateurs au moyen d'une adresse IPv4 et il devient donc considérablement plus difficile d'identifier des utilisateurs individuels*. Cette identification nécessiterait, de la part des opérateurs d'internet, qu'ils conservent ces données et qu'ils les communiquent aux forces de l'ordre. »*

7. Conclusion

L'utilisation des services et infrastructures d'internet à des fins terroristes est un défi international, auquel peu d'instruments internationaux sont spécifiquement consacrés. Des instruments comme la Convention de Budapest sont utiles pour la coopération policière contre le terrorisme et pour la collecte de preuves électroniques. Plusieurs difficultés subsistent, pour certaines d'ordre technologique, pour d'autres liées à la durée qu'entraînent les pratiques actuelles en matière d'entraide judiciaire.

Les questions de protection des données et de protection de la vie privée devraient toujours être prises en considération, comme la Cour européenne des droits de l'homme l'a indiqué dans l'affaire K.U. c. Finlande (requête n° 2842/02) :

https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf

« 49. (…) La prépondérance ayant été accordée à l'exigence de confidentialité, il n'a jamais été possible de procéder à une enquête efficace. Même si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. »

8. Recommandations au CODEXTER

Les membres du CODEXTER sont invités à prendre en considération les recommandations suivantes :

- Continuer de suivre étroitement la question du « terrorisme et internet » afin de traiter également cette question lorsqu'il analyse d'autres faits, tels que les combattants terroristes étrangers, l'entraînement pour le terrorisme, le financement du terrorisme et les terroristes agissant de manière isolée.

- Conformément à la Stratégie du Conseil de l'Europe sur la gouvernance de l'Internet 2016-2019, étudier la faisabilité d'une action conjointe avec les grandes entreprises d'internet par le biais d'une plate-forme qui sera mise en place dans le cadre de la Stratégie susmentionnée (paragraphe 13, e).

Le CODEXTER pourra naturellement identifier d'autres domaines pertinents lors de ses délibérations.

****

[i] Liste des conventions internationales relatives au terrorisme :

1 Convention pour la répression de la capture illicite d'aéronefs, signée à La Haye le 16 décembre 1970 ;

2 Convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, signée à Montréal le 23 septembre 1971 ;

3 Convention sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale, y compris les agents diplomatiques, adoptée à New York le 14 décembre 1973 ;

4 Convention internationale contre la prise d'otages, adoptée à New York le 17 décembre 1979 ;

5 Convention sur la protection physique des matières nucléaires, adoptée à Vienne le 3 mars1980 ;

6 Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, conclu à Montréal le 24 février 1988;

7 Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime, conclue à Rome le 10 mars 1988 ;

8 Protocole pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental, conclu à Rome le 10 mars 1988 ;

9 Convention internationale pour la répression des attentats terroristes à l'explosif, adoptée à New York le 15 décembre 1997 ;

10 Convention internationale pour la répression du financement du terrorisme, adoptée à New York le 9 décembre 1999 ;

11 Convention internationale pour la répression des actes de terrorisme nucléaire, adoptée à New York le 13 avril 2005.

[ii] https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

[iii] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[iv] http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

[v] https://en.wikipedia.org/wiki/Golden_Shield_Project

[vi] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59