COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

16 septembre 2016
Strasbourg, France

T-CY (2016)5
Provisoire

Comité de la Convention sur la cybercriminalité (T-CY)

# Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY

Rapport final du Groupe de travail du T-CY sur les preuves dans le cloud

www.coe.int/cybercrime

Contact
Alexander Seger
Secrétaire exécutif du Comité de la Convention sur la cybercriminalité (T-CY)
Direction générale des droits de l'homme et de l'Etat de droit
Conseil de l'Europe, Strasbourg, France
Tél. +33-3-9021-4506
Fax +33-3-9021-5650
Courriel alexander.seger@coe.int

# Table des matières

## Table des matières

# 1 Contexte et objet du présent rapport

1 A sa 12e réunion plénière, tenue les 2 et 3 décembre 2014, le Comité de la Convention sur la cybercriminalité (T-CY) a constitué un groupe de travail chargé d'examiner des solutions concernant l'accès de la justice pénale aux preuves stockées dans le cloud, notamment dans le cadre de l'entraide judiciaire (« Groupe de travail sur les preuves dans le cloud » - "*cloud Evidence Group*")[1].

2 Cette décision était motivée par la reconnaissance qu'avec la prolifération de la cybercriminalité et d'autres infractions impliquant des preuves électroniques, dans le contexte de l'évolution technologique et des incertitudes quant à la compétence juridique, des solutions complémentaires sont nécessaires pour permettre aux autorités judiciaires d'obtenir des preuves électroniques spécifiées dans le cadre d'enquêtes pénales spécifiques.

3 Le Groupe de travail sur les preuves dans le cloud doit présenter un rapport au T-CY assorti d'options et de recommandations d'actions futures d'ici décembre 2016. Ses travaux se fondent sur :

- les recommandations du rapport d'évaluation du T-CY sur les dispositions de la Convention de Budapest sur la cybercriminalité relatives à l'entraide judiciaire (document T-CY (2013)17rev)[2] ;
- les travaux du sous-groupe ad hoc sur l'accès transfrontalier aux données et la compétence[3] ;
- une description détaillée de la situation et des problèmes actuels ainsi que des nouveaux défis concernant l'accès de la justice pénale aux données dans le cloud et sur le territoire de juridictions étrangères.

4 Les solutions devraient s'inscrire dans le champ d'application de l'article 14 de la Convention de Budapest[4], c'est-à-dire couvrir des données spécifiées dans le cadre d'enquêtes pénales spécifiques. Elles ne porteront pas sur l'interception massive de données ni sur d'autres mesures à des fins de sécurité nationale.

5 Etant donné l'intérêt de l'Union européenne pour cette question, le Groupe de travail sur les preuves dans le cloud s'est donné pour objectif de travailler en étroite collaboration avec les institutions de l'UE et, plus particulièrement, avec la présidence néerlandaise de l'UE au cours de la première moitié de 2016[5].

---

[1] Document T-CY(2014)16 : Accès transfrontalier aux données et compétence : options concernant l'action future du T-CY (rapport du Groupe sur l'accès transfrontalier adopté à la 12e réunion plénière du T-CY en décembre 2014).

[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

[3] http://www.coe.int/fr/web/cybercrime/tb

[4] Article 14 – Portée d'application des mesures du droit de procédure
1 Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
b à toutes les autres infractions pénales commises au moyen d'un système informatique ;
c à la collecte des preuves électroniques de toute infraction pénale. »

[5] En juin 2016, le Conseil « Justice et affaires intérieures » de l'Union européenne a adopté un train de mesures visant à améliorer la justice pénale dans le cyberespace. Ces mesures sont inspirées du travail et des résultats préliminaires du Groupe de travail sur les preuves dans le cloud. http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09-criminal-activities-cyberspace/
Voir également les références à la nécessaire efficacité de l'accès aux preuves électroniques :
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_fr.pdf
http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/fr/pdf

6 Le présent document constitue le rapport final du Groupe de travail sur les preuves dans le cloud pour présentation au T-CY. Il résume les défis, les problèmes et les solutions définis par le Groupe de travail sur les preuves dans le cloud et comprend un ensemble de recommandations pour examen par le T-CY.

## Activités du Groupe de travail sur les preuves dans le cloud

| | |
|---|---|
| Strasbourg, 3 et 4 février 2015 | Réunion du Groupe de travail sur les preuves dans le cloud |
| Klingenthal, 6 et 7 mai 2015 | Réunion du Groupe de travail sur les preuves dans le cloud et finalisation des discussions relatives aux défis |
| Strasbourg, 15 et 16 juin 2015 | Réunion plénière du T-CY : présentation du document de réflexion sur les « Défis » |
| Strasbourg, du 17 au 19 juin 2015 | Conférence Octopus : atelier sur les preuves dans le cloud |
| La Haye, du 28 au 30 septembre 2015 | Réunion du Groupe de travail sur les preuves dans le cloud à EUROPOL avec des représentants de la Direction générale Migration et Affaires intérieures de la Commission européenne, du groupe de travail « Article 29 », d'EUROJUST, d'EUROPOL et de la Cour européenne de justice |
| Strasbourg, 30 novembre 2015 | Auditions de fournisseurs de service |
| Strasbourg, 1er et 2 décembre 2015 | Réunion plénière du T-CY : point sur le travail du Groupe de travail sur les preuves dans le cloud |
| Fribourg, du 7 au 9 février 2016 | Réunion du Groupe de travail sur les preuves dans le cloud à l'Institut Max-Planck |
| Amsterdam, 7 et 8 mars 2016 | Participation de certains membres du Groupe de travail sur les preuves dans le cloud et du Secrétariat du T-CY à la Conférence d'Amsterdam sur la compétence juridique dans le cyberespace, avec présentation des « problèmes et options » |
| Bruxelles, 24 et 25 avril 2016 | Réunion du Groupe de travail sur les preuves dans le cloud et échange de vues avec les fournisseurs de services et des représentants de la Commission européenne |
| Strasbourg, 3 mai 2016 | Finalisation d'un document d'information sur « La coopération avec les fournisseurs de service étrangers » |
| Strasbourg, 23 mai 2016 | Echange de vues avec des organisations oeuvrant pour la protection des données |
| Strasbourg, 24 et 25 mai 2016 | Réunion plénière du T-CY : présentation de propositions d'options et de recommandations |
| Strasbourg, du 12 au 14 septembre 2016 | Réunion du Groupe de travail sur les preuves dans le cloud et réunion informelle avec des membres du Parlement de l'Union européenne |
| Strasbourg, 14 et 15 novembre 2016 | Réunion plénière du T-CY : présentation du projet final de rapport pour examen par le T-CY |
| Strasbourg, du 16 au 18 novembre 2016 | Présentation des conclusions lors de la Conférence Octopus |

## Documents élaborés par le Groupe de travail sur les preuves dans le cloud

| | |
|---|---|
| T-CY(2015)10<br>26 mai 2015 | Défis qui se posent à la justice pénale en matière d'accès aux données stockées dans le cloud[6] |
| T-CY(2015)21<br>18 février 2016 | Application de l'article 18.1.b de la Convention de Budapest sur les « injonctions de produire » : compilation des réponses au questionnaire[7] |
| T-CY(2016)7<br>17 février 2016 | Accès de la justice pénale aux preuves électroniques dans le cloud – Synthèse informelle des problématiques et options à l'examen par |

[6] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053cb
[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a0873 (en anglais)

| | |
|---|---|
| | le Groupe de travail sur les preuves dans le cloud[8] |
| T-CY(2016)2<br>3 mai 2016 | Accès de la justice pénale aux données stockées dans le cloud : la coopération avec des fournisseurs de services « étrangers »[9] |
| T-CY(2015)16<br>4 mai 2016 | Projet de Note d'orientation n° 10 sur les injonctions de produire[10] |
| T-CY(2016)13<br>4 mai 2016 | Demandes urgentes de divulgation immédiate de données : compilation des réponses au questionnaire[11] |

[8] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064aaa4
[9] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d
[10] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651f03
[11] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f (en anglais)

# 2 Défis

7 En mai 2015, le Groupe de travail sur les preuves dans le cloud a publié un document de réflexion intitulé « Défis de l'accès de la justice pénale aux données stockées dans le cloud[12] » dans le but de faciliter les délibérations du T-CY, de la Conférence Octopus de 2015[13] et d'autres instances, de favoriser la coopération du secteur industriel et d'autres parties prenantes, ainsi que de dégager des solutions.

8 Les réflexions, affaires et rapports présentés ci-après étayent l'analyse des défis résumée dans le présent rapport.

## 2.1 Echelle et ampleur de la cybercriminalité, des dispositifs, des utilisateurs et des victimes

9 L'ampleur, la portée et les enjeux actuels de la cybercriminalité et des preuves électroniques (c'est-à-dire les preuves sous forme de données produites par ou stockées sur un système informatique) sont tels que la cybercriminalité est devenue une menace sérieuse pour les droits fondamentaux des individus, l'Etat de droit dans le cyberespace et les sociétés démocratiques. La cybercriminalité porte atteinte au droit à la vie privée et à la protection des données à caractère personnel autant qu'elle constitue une atteinte à la dignité et à l'intégrité des personnes, en particulier des enfants. La cybercriminalité porte atteinte à la liberté d'expression par des attaques contre des médias, des organisations de la société civile et des personnes, et à la démocratie par des attaques contre des gouvernements, des parlements et d'autres institutions démocratiques. Elle menace la stabilité démocratique lorsque les technologies de l'information et de la communication sont utilisées de façon abusive pour transmettre des messages xénophobes et racistes et contribuent à la radicalisation et au terrorisme. Enfin, elle menace la paix et la stabilité au niveau international, car les conflits militaires et les désaccords politiques s'accompagnent souvent de cyberattaques.

10 La cybercriminalité est tout sauf une problématique mineure : elle est une source de préoccupation majeure pour les gouvernements, les sociétés et les individus en raison de la dépendance aux technologies de l'information et de la communication, des milliards d'incidents qui se produisent sur les réseaux chaque année et des millions d'attaques quotidiennes perpétrées contre des systèmes informatiques et des données.

11 Des preuves en lien avec tout type d'infraction, y compris sans lien avec la cybercriminalité, sont désormais souvent conservées sous forme électronique sur des systèmes informatiques et relèvent généralement de compétences étrangères, inconnues, multiples ou changeantes. Les demandes internationales de données sont liées principalement à la fraude et à d'autres délits financiers, suivis des crimes violents et crimes graves, à savoir les meurtres, les agressions, le trafic illicite de personnes, la traite d'êtres humains, le trafic de stupéfiants, le blanchiment de capitaux, le terrorisme et son financement, l'extorsion et, en particulier, la pédopornographie et d'autres formes d'exploitation et d'abus sexuels à l'encontre d'enfants.

12 Tout porte à croire que l'ampleur de la cybercriminalité et des autres infractions impliquant des preuves électroniques va augmenter de manière significative dans les temps qui viennent.

---

12 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053cb

13 http://www.coe.int/en/web/cybercrime/octopus2015 (en anglais)

## 2.2 Garantir la prééminence du droit dans le cyberespace

13 La cybercriminalité, le nombre d'appareils électroniques, de services et d'utilisateurs (notamment d'appareils et de services mobiles) et, parallèlement, le nombre de victimes ont pris des proportions telles que seule une part infime des actes criminels et autres infractions perpétrés à l'aide d'un ordinateur et impliquant l'existence d'éléments de preuve électroniques donne lieu à une plainte et à des enquêtes. Les victimes ne peuvent, dans leur grande majorité, espérer que justice sera rendue. Cela pose problème du point de vue de la prééminence du droit dans le cyberespace et soulève la question de savoir si les gouvernements sont à même de satisfaire à l'obligation qui leur est faite de préserver la société de la délinquance et de protéger les droits des victimes[14].

14 Comme expliqué plus haut, les infractions perpétrées dans le monde physique impliquent de plus en plus des éléments de preuve électroniques. La prééminence du droit est donc menacée non seulement dans le cyberespace, mais également dans le monde physique. En définitive, le fait que la capacité de mener des enquêtes et de défendre la sûreté publique et les droits de l'homme soit de plus en plus restreinte aura plusieurs conséquences : d'une part, le recours à l'autodéfense ou l'absence de justice pour les victimes ; d'autre part, l'accumulation d'argent et de pouvoir par les criminels, et la corruption de gouvernements démocratiques.

15 La principale menace pesant sur la prééminence du droit est la difficulté de garantir que les données pourront être utilisées comme éléments de preuve lors de procédures pénales :

- les défis techniques à ce sujet sont notamment en lien avec les réseaux virtuels privés, les anonymiseurs (TOR), le cryptage, la VoIP ou la traduction d'adresses réseau à grande échelle (CGN) au cours de la transition IPv4 vers IPv6. Ces éléments préoccupants ne relèvent pas de la compétence du Groupe de travail sur les preuves dans le cloud ;

- les défis juridiques et juridictionnels sont majoritairement liés à l'informatique dans le cloud.

## 2.3 Informatique dans le cloud, territorialité et compétence[15]

16 L'informatique dans le cloud désigne le stockage de données sur un appareil spécifique ou dans un réseau fermé mais partagé entre différents services, fournisseurs, lieux ou, souvent, juridictions. Plusieurs questions se posent :

- l'indépendance par rapport au lieu est une caractéristique essentielle de l'informatique dans le cloud. En conséquence :

  - dans bien des cas, les instances pénales ne savent pas trop où sont conservées les données ni de quel régime juridique elles relèvent. Un fournisseur de services peut avoir son siège dans un pays donné et relever juridiquement du ressort d'un deuxième, alors que les données sont stockées dans un troisième. Les données peuvent être recopiées en miroir dans plusieurs pays ou être relocalisées dans d'autres pays. Si le lieu où sont conservées les données détermine la compétence, il n'est pas exclu qu'un fournisseur de services dans le cloud déplace systématiquement les données pour empêcher l'accès de la

[14] Concernant l'obligation des gouvernements de protéger les individus des infractions, notamment par l'intermédiaire du droit pénal, voir Cour européenne des droits de l'homme dans l'affaire K.U. c. Finlande (en anglais uniquement) : https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf

[15] Pour une version plus détaillée et annotée de cette section, voir le rapport « Défis » de mai 2015 : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053cb

justice pénale. Il se peut aussi que le fournisseur ne sache pas vraiment où se trouvent les données.

- Même si, en théorie, il est toujours possible de situer l'endroit où se trouvent des données lorsqu'elles sont conservées sur des serveurs dans le cloud, il est très difficile de savoir clairement quelles règles s'appliquent pour assurer un accès légal aux autorités judiciaires. On peut considérer que la compétence est déterminée par le lieu où se trouve le siège du fournisseur de services ou de son sous-traitant, mais aussi par le lieu où se trouvent les données et le serveur, ou encore par la législation de l'Etat dans lequel le suspect s'est abonné à un service, voire le lieu où se trouve le suspect ou la nationalité de ce dernier.
- Dans de nombreux cas, on ne sait pas clairement si un fournisseur de services dans le cloud est responsable du « traitement » ou du « sous-traitement » des données d'un utilisateur et, de fait, quelles règles s'appliquent.
- D'autres questions se posent en matière de compétence, par exemple lorsque le propriétaire des données est inconnu ou que les données sont conservées via des systèmes de co-hébergement transnationaux.

▪ Un fournisseur de services peut relever de différents niveaux de compétence à la fois pour divers aspects juridiques liés à ses services. Par exemple :

- à des fins de protection des données, sur le territoire des Etats membres de l'Union européenne, la compétence semble être déterminée par le lieu où se trouve le responsable du traitement des données (même si celui-ci se fait à l'extérieur de l'Union européenne) ou par le lieu de traitement des données des personnes concernées situé dans l'Union européenne (même lorsque le responsable du traitement ou du sous-traitement n'est pas établi dans l'Union européenne) si le traitement est en lien avec l'offre de biens ou de services aux personnes concernées dans l'Union européenne[16] ;
- à des fins fiscales, la compétence semble ne pas être déterminée par le lieu où se trouvent le siège international, les serveurs ou les responsables du traitement des données, mais par plusieurs autres critères, tels que le lieu où se trouve la filiale qui exerce les activités ;
- concernant la protection du consommateur, le lieu où se trouve le consommateur semble déterminant ;
- pour ce qui est des droits de propriété intellectuelle dans le cadre d'affaires civiles, le lieu où se trouve la société semble déterminer la compétence, tandis que pour les droits de propriété intellectuelle dans le cadre d'affaires pénales, le lieu où se trouve l'auteur de l'infraction peut être déterminant ;
- dans des affaires anti-trust, il est recommandé aux autorités de la concurrence de l'Union européenne d'étendre les recherches menées sur l'ordinateur d'une entreprise ou de sa filiale dans l'Union européenne aux ordinateurs relevant d'autres juridictions dans le but de collecter des éléments de preuve ;
- les fournisseurs de services peuvent mettre en place des ententes commerciales en confiant à un tiers la responsabilité de leurs données, de manière à se protéger contre toute procédure juridique ;
- ils peuvent aussi s'organiser pour donner l'impression de ne pas avoir de siège ni de site physique afin de ne relever d'aucune juridiction.

▪ Le partage et la mise en commun des ressources sont une caractéristique essentielle de l'informatique dans le cloud. Les services proposés dans le cloud peuvent combiner

[16] Voir l'article 3 du Règlement général sur la protection des données et l'article 4 de la Directive 95/46/CE actuellement en vigueur.

plusieurs modèles de services (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)). Dans ces cas-là, on ne sait pas clairement quel fournisseur détient ou traite tel ou tel type de données (données relatives aux abonnés, au trafic et au contenu) et à qui il convient d'adresser une injonction de produire.

- Les fournisseurs de services dans le cloud peuvent décider que les décisions de justice soient dirigées contre les propriétaires des données et non contre eux. Cela pousse généralement les services répressifs à demander des comptes à plusieurs entreprises ou à déterminer si une entreprise est effectivement responsable du traitement des données tout en évitant que la cible (qui peut être l'entreprise responsable du traitement des données) ne détruise les données dès lors qu'elle a connaissance de l'enquête.

- Il est fréquent que l'on ne sache pas clairement si les données sont stockées ou si elles transitent et, par conséquent, si les injonctions de produire, la perquisition et la saisie des données informatiques, l'interception ou la collecte en temps réel des données doivent être exécutées.

- On ne sait pas toujours clairement si les différents types de services dans le cloud sont considérés et réglementés comme des « services de communication électronique » ou comme des « services de la société de l'information », ce qui a une incidence sur le type de compétences procédurales et les conditions applicables.

- Pour ce qui est des interceptions (obtention de contenu au titre des articles 21 et 34 de la Convention de Budapest), des problèmes spécifiques se posent, par exemple :

  - dans de nombreux cas, une injonction de tribunal adressée à un fournisseur de services dans un pays pour intercepter une communication électronique entre deux suspects sur son territoire et/ou entre ses ressortissants est souvent inexécutable en temps réel du fait que le serveur où l'interception doit être effectuée relève de la compétence d'un autre pays ou que la communication passe par un pays étranger. Il est peu probable que les autorités étrangères répondent à une demande d'entraide judiciaire en temps réel, compte tenu de la durée des procédures et des conditions d'interception dans le pays concerné, excepté si des procédures d'urgence sont en place. Concernant les Etats-Unis, les autorités fédérales ne peuvent pas obtenir du contenu en temps réel pour les autorités étrangères ;
  - une injonction de tribunal peut être délivrée pour intercepter la communication d'un suspect du pays concerné. Cependant, lorsque le suspect est en fuite, qu'il se rend dans un autre pays ou circule entre différents pays, il peut s'avérer difficile de savoir si l'interception est possible sur le plan juridique.

- La nature non localisée de l'informatique dans le cloud pose problème pour les perquisitions et les investigations informatiques forensiques à chaud du fait de l'architecture du cloud (mutualisation, distribution et séparation des données) et des enjeux juridiques liés à l'intégrité et à la validité de la collecte des données, au contrôle des éléments de preuve, à la propriété des données et à la compétence.

## 2.4 Entraide judiciaire

17 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 sur la Cybercriminalité (T-CY) a mené une évaluation du fonctionnement des dispositions concernant l'entraide judiciaire[17]. 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.

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

19 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 preuve stockés dans le cloud.

## 2.5 Questions

20 Dans ses conclusions, le document relatif aux défis soulevait un certain nombre de questions relatives à la compétence et à l'entraide judiciaire :

- quel gouvernement serait le destinataire d'une demande légale de données adressée par un pays victime d'une cyber-attaque dans le cloud dont le pays d'origine n'est pas clairement identifié, lorsque le responsable du traitement des données est masqué par différents niveaux de fournisseurs de services et lorsque les données circulent et sont fragmentées ou reproduites en miroir dans plusieurs pays ?

- Quel élément détermine la compétence d'application de la législation pénale : le lieu où se trouvent les données ? La nationalité du propriétaire des données ? Le lieu où se trouve le propriétaire des données ? La nationalité du propriétaire des données ? Le lieu où se trouve le responsable du traitement des données ? Le lieu où se trouve le siège du fournisseur de services dans le cloud, ou sa filiale ? Le pays où un fournisseur de services dans le cloud offre ses prestations ? La législation du pays où le propriétaire des données s'est abonné à un service ? Le pays des autorités judiciaires ? L'importance de l'activité du fournisseur de services dans le pays ?

- Qu'entend-on par « offrant des prestations sur le territoire de la Partie » (article 18.1.b de la Convention de Budapest)[18] ?

- Si une injonction d'un tribunal national autorise l'interception d'une communication entre deux ressortissants du pays ou autres personnes sur son territoire, pourquoi l'entraide judiciaire ne serait-elle pas requise alors que, techniquement, le fournisseur procéderait

[17] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

[18] Article 18 – Injonction de produire
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; et
b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

à l'interception sur un serveur installé dans un pays étranger ? Dans quelle mesure la souveraineté de ce pays serait-elle affectée ? Dans quelle mesure les droits de la défense ne seraient-ils pas protégés ? La situation serait-elle la même pour les injonctions de produire concernant les données relatives au contenu ?

- Est-il réaliste d'envisager que le nombre de demandes d'entraides judiciaires adressées, reçues et traitées puisse être multiplié par cent, mille ou dix mille ? Les gouvernements ont-ils la capacité d'augmenter considérablement les ressources disponibles pour assurer un traitement efficient des demandes d'entraide judiciaire au niveau des autorités centrales compétentes, mais aussi des tribunaux locaux et des services de poursuite et de police où les demandes sont préparées et exécutées ?

- Quel délai serait raisonnable pour obtenir des données auprès d'une autorité étrangère ? Ce délai pourrait-il être défini dans le cadre d'un accord contraignant ?

- L'élaboration d'un régime simplifié pour les données relatives aux abonnés, par exemple la divulgation rapide de données, est-elle envisageable ?

- Quelles autres solutions juridiquement contraignantes à l'échelle internationale pourraient être envisagées pour permettre un accès efficient de la justice pénale à des données précises dans des pays étrangers ou non identifiés dans le cadre d'enquêtes pénales spécifiques[19] ?

21 Les problèmes spécifiques définis et les solutions proposées par le Groupe de travail sur les preuves dans le cloud pourraient permettre de répondre à ces questions.

[19] Voir, par exemple les recommandations 19 à 24, page 141 de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

# 3 Questions spécifiques restant à aborder

22 Le Groupe de travail du T-CY Preuves dans le cloud estime que les questions spécifiques suivantes doivent être abordées.

## 3.1 Entraide judiciaire

23 Lorsque des éléments de preuve sont stockés dans des juridictions étrangères, l'entraide judiciaire en matière pénale est le principal moyen de les obtenir. En 2013 et 2014, le T-CY a réalisé une évaluation détaillée des dispositions relatives à l'entraide judiciaire de la Convention de Budapest. En décembre 2014, il a adopté un rapport contenant un ensemble de recommandations visant à améliorer l'efficience de l'entraide judiciaire[20]. Du point de vue du Groupe de travail sur les preuves dans le cloud, cette évaluation et les recommandations correspondantes restent valables.

24 Le rapport conclut que, dans l'ensemble[21] :

> une entraide accélérée est l'une des conditions les plus importantes pour des mesures efficaces contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques, étant donné la nature transnationale et volatile de ces dernières. En pratique, toutefois, les procédures liées à l'entraide sont jugées trop complexes, prenant trop de temps et mobilisant trop de ressources, et par là même étant par trop efficientes.
> (…)
> 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 pour lesquels la preuve est de nature électronique.
> (…)
> Or, les Parties semblent ne pas mettre pleinement à profit les opportunités offertes par la Convention de Budapest sur la cybercriminalité et d'autres accords afin de parvenir à une entraide efficace en matière de cybercriminalité et de preuves électroniques.

25 Il conclut par ailleurs que toutes les catégories de données ne sont pas demandées avec la même fréquence et le même niveau d'urgence :

> Pour ce qui est du type d'informations demandées, les informations concernant les abonnés ressortent comme étant les informations les plus fréquemment demandées. Le très grand nombre de demandes pour les données de ce type grève lourdement les autorités responsables du traitement et de l'exécution des DEJ, outre qu'il ralentit, voire empêche, les enquêtes criminelles. On pourrait donc penser que si l'on trouvait des solutions aux difficultés posées par les informations concernant les abonnés, les DEJ en seraient plus efficientes.

26 En décembre 2014, le T-CY a donc adopté un ensemble de recommandations visant à rendre la procédure d'entraide judiciaire concernant la cybercriminalité et les éléments de preuve électroniques plus efficiente en mettant davantage en pratique les dispositions existantes de la Convention de Budapest sur la cybercriminalité et d'autres accords, mais également en proposant d'autres solutions[22].

[20] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d
[21] Voir la page 136 du rapport : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d
[22] Voir pages 139 à 141 du rapport : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

27 Les trois recommandations ci-après sont données à titre d'exemple.

- Les Parties devraient pleinement mettre en œuvre les pouvoirs en matière de conservation prévus dans la Convention de Budapest (Recommandation 1), suivre l'efficience du processus d'entraide (Recommandation 2), affecter davantage de personnel et du personnel mieux formé aux technologies ainsi que davantage de ressources pour les demandes d'entraide (MLA) (recommandations 3 et 4), renforcer le rôle et les capacités des points de contact 24/7 (Recommandation 5), établir des procédures d'urgence (Recommandation 8), etc.

- Le Conseil de l'Europe devrait, par ses projets de renforcement des capacités, élaborer des outils et des formulaires modèles standardisés et plurilingues disponibles en lignes pour les demandes effectuées au titre de l'article 31 relatives aux données stockées (Recommandations 17 et 18).

- Les Parties devraient envisager, par exemple au moyen d'un Protocole additionnel à la Convention de Budapest, de permettre la divulgation rapide des données relatives aux abonnés (Recommandation 19), l'introduction d'injonctions de produire internationales (Recommandation 20), la coopération directe entre autorités judiciaires (Recommandation 21), l'obtention directe d'informations auprès de fournisseurs de services étrangers (Recommandation 22), la conduite d'enquêtes conjointes et/ou l'établissement d'équipes communes d'enquête entre les Parties (Recommandation 23), et la possibilité d'envoyer des demandes en anglais (Recommandation 24).

28 Le T-CY a commencé un travail de suivi des recommandations 1 à 18[23]. Les recommandations 19 à 24 et la Recommandation 8 sur les situations d'urgence[24] sont abordées ci-après, parallèlement aux options pouvant être mises en œuvre.

## 3.2 Distinguer les différents types de données recherchées

29 Trois types de données peuvent être nécessaires aux fins d'enquêtes pénales, à savoir :

- les « données relatives aux abonnés[25] », c'est-à-dire les informations permettant d'identifier l'utilisateur d'une adresse IP spécifique ou, à l'inverse, les adresses IP utilisées par une personne précise. Les données relatives aux abonnés comprennent également les données tirées de bureaux d'enregistrement sur les déposants de noms de domaines ;

- les « données relatives au trafic[26] », c'est-à-dire les fichiers où sont enregistrées les activités du système d'exploitation d'un ordinateur ou d'autres logiciels ou les

[23] Voir la 15e Plénière du T-CY en mai 2016 : http://www.coe.int/fr/web/cybercrime/t-cy-plenaries

[24] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f (en anglais)

[25] Le terme « données relatives aux abonnés » est défini à l'article 18.3 de la Convention de Budapest :
« 3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service ».

[26] selon la définition donnée à l'article 1.d de la Convention de Budapest :
« d. « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un

communications entre des ordinateurs, en particulier lorsqu'il s'agit de l'expéditeur ou du destinataire de messages ;

- les « données relatives au contenu », par exemple les messages électroniques, images, films, musique et documents[27]. Il y a lieu de faire la distinction entre les données relatives au contenu « conservées », c'est-à-dire les données déjà disponibles sur un système informatique, et les données relatives au contenu « futures », qui ne sont pas encore disponibles et qui devront être obtenues en temps réel.

30 Les données relatives aux abonnés sont les informations les plus fréquemment recherchées dans les enquêtes pénales à l'échelle nationale et internationale, pour ce qui est de la cybercriminalité et des preuves électroniques, comme cela a été mis en avant par les Parties dans le rapport d'analyse du T-CY de 2014. Sans ces informations, il est souvent impossible de mener une enquête. Il est donc essentiel d'aborder la question de l'obtention des données relatives aux abonnés.

31 Les données relatives aux abonnés sont généralement considérées comme étant moins sensibles, du point de vue du respect de la vie privée, que les données relatives au trafic et celles relatives au contenu. Par conséquent, la plupart des systèmes de droit pénal définissent des garanties strictes pour l'accès au contenu par les services répressifs, notamment en ce qui concerne l'interception des communications.

32 Les données relatives au trafic sont considérées comme sensibles, comme le souligne par exemple la Cour européenne de justice à propos de la question de la conservation des données[28].

33 Les données relatives aux abonnés sont généralement détenues par des fournisseurs de services du secteur privé, et les services d'enquête les obtiennent habituellement grâce à des injonctions de produire[29]. La procédure découlant d'une injonction de produire s'immisce moins dans les droits de la personne et les intérêts des tiers que la recherche et la saisie d'ordinateurs ou l'interception de communications.

34 Par conséquent, et puisque la Convention de Budapest fait la distinction entre les données relatives aux abonnés, les données relatives au trafic et les données relatives au contenu, le Groupe de travail sur les preuves dans le cloud estime que la mise en place d'un régime distinct pour l'accès aux informations relatives aux abonnés favorisera grandement l'efficience de l'entraide judiciaire en matière de cybercriminalité et d'éléments de preuve électroniques. L'article 18 de la Convention de Budapest pose les bases juridiques pour cela.

---

système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent ».

[27] D'après le paragraphe 209 du Rapport explicatif de la Convention de Budapest :
« Les « données relatives au contenu » ne sont pas définies dans la Convention, mais désignent le contenu informatif de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic) ».

[28] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf
« La Cour constate tout d'abord que les données à conserver permettent notamment de savoir avec quelle personne et par quel moyen un abonné ou un utilisateur inscrit a communiqué, de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu et de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée. Ces données, prises dans leur ensemble, sont susceptible de fournir des indications très précises sur la vie privée des personnes dont les données sont conservées, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés.
La Cour estime qu'en imposant la conservation de ces données et en en permettant l'accès aux autorités nationales compétentes, la Directive s'immisce de manière particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ».

[29] Voir l'article 18 de la Convention de Budapest.

> Article 18 – Injonction de produire
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
> a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et
> b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

35 Cependant, il conviendrait de résoudre plusieurs problèmes dans ce contexte :

- Toutes les Parties à la Convention de Budapest n'appliquent pas les mêmes règles concernant l'obtention de données relatives aux abonnés. En 2014, le T-CY a examiné les procédures d'obtention des données relatives aux abonnés[30] et a conclu que, si la plupart des Parties ayant répondu au questionnaire font la distinction entre les notions de « données relatives aux abonnés » et « données relatives au trafic » :

  - « Dans la plupart des Parties ayant répondu au questionnaire, il apparaît que les conditions requises pour l'obtention d'informations relatives aux abonnés sont semblables ou similaires à celles requises pour l'obtention de données relatives au trafic, notamment si les données relatives aux abonnés sont associées à une adresse IP dynamique[31]. Dans plus de la moitié des Parties en question, une autorisation judiciaire est nécessaire pour obtenir des informations relatives aux abonnés ; dans d'autres, le ministère public ou un haut responsable des services répressifs habilité peut ordonner la production de ces informations.
  - Dans d'autres Parties, les conditions requises pour l'obtention des informations relatives aux abonnés sont moins exigeantes que celles requises pour les données relatives au trafic et la production d'informations relatives aux abonnés peut être ordonnée par la police ou le ministère public. »

- Cette diversité des approches bride les enquêtes nationales et la coopération internationale. Le rapport, adopté par le T-CY en décembre 2014, recommandait 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 » et « d'encourager les Parties à tenir compte des observations du présent rapport lors de la refonte de leur législation interne ».

---

30 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044e292

31 Certaines Parties ne font pas la distinction entre l'accès aux données relatives aux abonnés (en particulier pour les adresses IP dynamiques) et l'accès aux données relatives au trafic, sans doute parce que plusieurs instruments du droit européen ne font pas la distinction entre ces deux catégories. Voir par exemple les catégories de données devant être conservées au titre de l'article 5 de l'ancienne Directive 2006/24/CE relative à la conservation des données (http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32006L0024&from=FR). Cette Directive a été déclarée invalide par la Cour de justice européenne en 2014.
La Directive vie privée et communications électroniques définissait les « données relatives au trafic » comme suit :
« Article 2 (b) « données relatives au trafic » : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ». Cette Directive ne proposait pas de définition distincte des « données relatives aux abonnés », qui semblent être en partie intégrées dans le terme « données relatives au trafic » (Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML Cette Directive a été révisée en 2009 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:Fr:PDF)

36 Le Groupe de travail sur les preuves dans le cloud souligne également que le Conseil « Justice et affaires intérieures » de l'Union européenne, dans ses « Conclusions sur l'amélioration de la justice pénale dans le cyberespace » adoptées le 9 juin 2016[32], a indiqué ce qui suit :

> « L'amélioration de la coopération avec les fournisseurs de services ou toute autre solution comparable permettant une divulgation rapide des données doit être envisagée ; une procédure juridique moins rigoureuse devrait être prévue pour obtenir des catégories de données spécifiques, notamment les données relatives aux abonnés ».

37 Cette conclusion implique de faire la distinction entre plusieurs catégories de données dans la législation nationale et dans la réglementation relative à l'accès à chaque catégorie de données et à leur divulgation, notamment pour ce qui est des données relatives aux abonnés, par opposition aux données relatives au trafic.

38 Internet n'ayant aucune frontière physique, les données relatives aux abonnés nécessaires à une enquête peuvent être détenues par un fournisseur de services « offrant des prestations sur le territoire » de la Partie, bien que les informations puissent en fait être stockées sur des serveurs situés dans d'autres juridictions[33]. Le Groupe de travail sur les preuves dans le cloud estime qu'une interprétation par la logique de l'article 18.1.b de la Convention de Budapest offre une solution. Les autorités compétentes d'une Partie devraient pouvoir demander des données relatives aux abonnés à un fournisseur de services offrant un service sur son territoire quels que soient les lieux où ces données sont stockées et où son siège est situé. Cette condition est abordée plus loin dans une partie distincte.

[32] http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09-criminal-activities-cyberspace/
[33] Par exemple, Google possède également des centres de données en Europe (https://www.google.com/about/datacenters/inside/locations/index.html), Microsoft possède « plus de 100 centre de données », notamment à Amsterdam et à Dublin http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf (en anglais), et Facebook dispose d'un centre de données en Suède https://www.facebook.com/LuleaDataCenter (en anglais)

## 3.3 « Disparition du lieu »

39 L'entraide judiciaire suppose de connaître le lieu où se situent les données, et qu'il est possible de savoir à quel Etat et à quelle autorité compétente la demande doit être envoyée.

40 Dans le contexte de l'informatique dans le cloud, ce n'est généralement pas le cas, comme l'explique la partie du présent rapport intitulée « Informatique dans le cloud, territorialité et compétence » :

- dans bien des cas, les instances pénales ne savent pas vraiment où sont conservées les données ni de quel régime juridique elles relèvent. Un fournisseur de services peut avoir son siège dans un pays et relever du ressort d'un deuxième pays, alors que les données sont stockées dans un troisième. Les données peuvent être recopiées en miroir dans plusieurs pays ou être relocalisées dans d'autres pays. Si le lieu où sont conservées les données détermine la compétence, il n'est pas exclu qu'un fournisseur de services dans le cloud déplace systématiquement les données pour empêcher que la justice pénale y accède.

- Même si, en théorie, il est toujours possible de localiser l'endroit où se trouvent des données lorsqu'elles sont conservées sur des serveurs dans le cloud, il est très difficile de savoir clairement quelles sont les règles qui s'appliquent pour assurer un accès légal aux autorités judiciaires. On peut estimer que la compétence est déterminée par le lieu où se trouve le siège du fournisseur de services ou de son sous-traitant, par le lieu où se trouvent les données et le serveur, par la législation de l'Etat dans lequel le suspect s'est abonné à un service, ou encore par le lieu où se trouve le suspect ou sa nationalité.

41 Ainsi, par exemple,

- même si une ferme de serveurs est située sur le territoire d'un Etat, les autorités de ce dernier ne disposent pas d'indications suffisantes montrant que les données recherchées se trouvent effectivement sur les serveurs de cette ferme pour justifier un mandat de perquisition. Même avec un mandat de perquisition, elles pourraient ne pas pouvoir accéder aux données du fait d'un cryptage, dont les clés peuvent être détenues par une personne morale ou un individu se trouvant dans une autre juridiction ;

- lorsque l'origine d'une attaque n'est pas connue de la justice pénale ou qu'elle lui est dissimulée, des techniques de traçage peuvent orienter les enquêteurs vers des routeurs et des serveurs situés dans des juridictions inconnues ;

- lorsqu'un ordinateur situé sur une scène de crime ou appartenant à une personne faisant l'objet d'une enquête est en état de fonctionnement et allumé, les autorités pénales pourraient techniquement avoir accès aux données (y compris celles stockées sur des serveurs dans le cloud) sans connaître la juridiction où se trouve le serveur et où sont stockées les données.

42 Le principe de la territorialité détermine généralement la compétence des services répressifs. D'après ce principe, aucun Etat ne peut étendre sa juridiction au-delà des limites du territoire d'un autre Etat souverain[34]. La question de l'accès de la justice pénale à des données stockées sur des serveurs ou des ordinateurs situés dans une juridiction étrangère, sans la participation des autorités de cette juridiction, est préoccupante.

[34] Voir l'Affaire du « Lotus » (France c. Turquie), Cour permanente de justice internationale, Série A, nº 10
Voir également la page 10 du rapport du Groupe sur l'accès transfrontalier :
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044e8c0

43 Cependant, dans les situations « d'absence (de la connaissance) du lieu », le principe de la territorialité est difficile à mettre en œuvre, en particulier lorsqu'il doit s'appuyer sur le lieu où se trouvent les données recherchées.

44 L'article 32b de la Convention de Budapest sur la cybercriminalité offre une solution applicable uniquement à un nombre limité de situations, comme expliqué dans la Note d'orientation adoptée en décembre 2014 par le T-CY[35]. Celle-ci donne deux exemples :

- le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services, ou une personne peut stocker délibérément des données dans un autre pays. Cette personne peut récupérer les données et, pourvu qu'elle y soit juridiquement habilitée, elle peut les communiquer de son propre gré aux services d'enquête ou leur permettre d'y accéder, tel que prévu à l'article 32b.

- Un individu soupçonné de trafic de drogues est arrêté dans le respect des procédures alors que sa messagerie électronique est ouverte sur sa tablette, son smartphone ou un autre appareil, révélant éventuellement des preuves de délit. Si le suspect autorise de son propre gré la police à accéder à son compte et si celle-ci est certaine que les données sont localisées dans un autre Etat partie, elle peut y avoir accès en vertu de l'article 32b.

45 Comme le T-CY l'a précédemment fait remarquer, ces restrictions et l'absence de cadre juridique international clair, efficace et concret font que les gouvernements se tournent de plus en plus vers des solutions unilatérales. Dans le cadre d'une enquête pénale, l'accès par les services répressifs aux données stockées non seulement sur l'appareil du suspect mais également sur des dispositifs connectés comme la messagerie électronique ou un compte de services dans le cloud semble être une pratique très répandue, lorsque l'appareil est allumé ou que les informations d'identification ont été légalement obtenues, même si l'on sait que la connexion se fera vers un pays étranger.

46 Afin de réduire les risques pour les relations entre Etats et de défendre les droits de la personne, notamment pour garantir leur sécurité, il faut mettre en place un cadre international commun pour l'accès transnational aux données.

47 Le lieu où se trouve la victime au moment de l'infraction sur le territoire d'une Partie peut aussi justifier la compétence et, au besoin, l'accès transfrontalier (unilatéral) aux données, dans des limites ayant fait l'objet d'un accord.

48 Par exemple, si une personne morale ou physique qui fait l'objet d'une enquête est présente sur le territoire et donc dans la juridiction d'une instance pénale donnée, celle-ci pourrait être en mesure d'accéder légalement aux données possédées ou contrôlées par la personne ou de lui enjoindre de produire ces données, y compris lorsque celles-ci sont transfrontalières.

49 A ce propos, le Groupe de travail sur les preuves dans le cloud a examiné la doctrine de la législation antitrust de l'UE (Affaires *ICI* 48/69 et *Woodpulp* 89/85) et a relevé que la Commission européenne recommande que les autorités de la concurrence de l'Union européenne aient la possibilité d'accéder à des serveurs situés n'importe où dans le monde afin de collecter des éléments de preuve dans le cadre de procédures antitrust[36] :

[35] https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)7F_REV_GN3_transborder_V11.pdf
[36] Recommandation du European Competition Network sur la capacité de collecter des éléments de preuves numériques, y compris grâce à l'analyse forensique (en anglais) http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

5. La pratique montre qu'une entreprise peut utiliser, stocker ou avoir accès à des informations relatives à une activité commerciale sur des serveurs externes ou d'autres dispositifs de stockage, tels que les services dans le cloud (stockage en réseau sur des serveurs virtuels multiples) qui se trouvent hors du territoire sur lequel l'autorité de la concurrence concernée est compétente ou à l'extérieur de l'Union européenne. Il est important pour les autorités d'être habilitées à récolter, au cours de leur inspection, des informations numériques auxquelles l'entreprise ou la personne dont les locaux sont inspectés a accès, quel que soit le lieu où elles sont stockées, y compris sur des serveurs ou d'autres dispositifs de stockage se trouvant hors du territoire sur lequel l'autorité de la concurrence est compétente ou à l'extérieur de l'Union européenne.

Il est recommandé ce qui suit :

1. Toutes les autorités devraient être habilitées, de manière efficace et efficiente, à collecter des éléments de preuve électroniques, notamment ceux obtenus après une analyse forensique, une inspection des locaux commerciaux et non commerciaux, une demande de renseignements et grâce à d'autres outils d'enquête. A cette fin, les autorités devraient être en mesure de collecter l'ensemble des renseignements sous format numérique en lien avec l'entreprise ou les entreprises faisant l'objet d'une enquête, quels que soient le dispositif sur lequel ils sont stockés et la technologie employée. Les autorités devraient également pouvoir collecter des informations numériques en réalisant des copies numériques, notamment des images forensiques, des données détenues et/ou par l'intermédiaire de la saisie de dispositifs de stockage.

2. La capacité de collecter des éléments de preuve numériques, notamment celles obtenues après analyse forensique, comme établi dans la Recommandation 1, devrait comprendre le droit d'avoir accès aux renseignements disponibles sur la personne morale ou l'individu dont les locaux font l'objet d'une inspection et ayant un lien avec l'entreprise visée par une enquête.

50 Le cadre régissant l'accès transfrontalier aux données devra définir les conditions et les garanties correspondantes afin de protéger les droits individuels et d'éviter tout préjudice à l'encontre des pouvoirs ou droits d'autres gouvernements et de leurs ressortissants (en vertu de la définition de la notion de « courtoisie »).

51 Des discussions sont en cours au sein de l'Union européenne pour trouver des solutions à « la disparition du lieu ». Le Conseil « Justice et affaires intérieures » du Conseil de l'Europe, dans le document « Conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace », adopté le 9 juin 2016[37], a indiqué ce qui suit :

> La réglementation encadrant la compétence d'exécution devrait être révisée
> (…) lorsque le cadre existant n'est pas suffisant, par exemple lorsque plusieurs systèmes d'informations sont utilisés simultanément dans de multiples juridictions pour commettre une seule infraction, ou lorsque des éléments de preuve pertinents se déplacent d'une juridiction à l'autre dans un court laps de temps, ou lorsque des méthodes complexes sont utilisées pour dissimuler le lieu où se trouvent des éléments de preuve ou l'infraction, entraînant la « disparition du lieu »[38].

[37] http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09-criminal-activities-cyberspace
[38] Depuis, la Commission européenne a réalisé une étude auprès des Etats membres de l'UE (en anglais) : https://ec.europa.eu/eusurvey/runner/eevidence

## 3.4 Fournisseurs de services dont le siège est situé sur le territoire d'un État ou offrant un service sur ce territoire

52 Comme indiqué plus haut, l'un des principaux défis de l'informatique dans le cloud est lié au fait qu'on ne sait jamais vraiment où se trouvent les données, qui souvent sont diffusées ou se déplacent entre différents services, fournisseurs, lieux et juridictions, alors que les compétences en matière d'application de la loi sont généralement définies par le territoire.

53 Une autorité de justice pénale peut donc établir sa compétence d'exécution en se concentrant sur le lieu où se trouve l'ordinateur ou le dispositif de stockage (cette possibilité est couverte par les dispositions de l'article 19 de la Convention de Budapest sur la recherche et la saisie), ou sur le lieu où se trouve la personne morale ou l'individu (y compris le fournisseur de services) qui possède ou qui contrôle les données recherchées[39]. Ce cas est couvert par l'article 18 relatif aux injonctions de produire :

> Article 18 – Injonction de produire
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
>
> a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; et
>
> b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
>
> 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
>
> 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de

[39] Etant donné le caractère instable du lieu où se trouvent les données, la compétence est généralement définie selon le lieu où se situe la personne possédant les données ou exerçant un contrôle sur celles-ci, et non selon le lieu où se trouvent les données ou les systèmes informatiques. Par exemple, la Directive de l'Union européenne 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union du 6 juillet 2016 prévoit ce qui suit concernant la compétence :

« Article 18 Compétence et territorialité
1. Aux fins de la présente Directive, un fournisseur de services numérique est considéré comme relevant de la compétence de l'Etat membre dans lequel il a son établissement principal. Un fournisseur de services numérique est réputé avoir son établissement principal dans un Etat membre lorsque son siège social se trouve dans cet Etat membre.
2. Un fournisseur de services numérique qui n'est pas établi dans l'Union mais fournit des services visés à l'annexe III à l'intérieur de l'Union désigne un représentant dans l'Union. Le représentant est établi dans l'un des Etats membres dans lesquels les services sont fournis. Le fournisseur de services numérique est considéré comme relevant de la compétence de l'Etat membre dans lequel le représentant est établi.
3. La désignation d'un représentant par le fournisseur de services numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de services numérique lui-même. »
Le considérant 64 est formulé comme suit :
« La compétence dont relèvent les fournisseurs de service numérique devrait être attribuée à l'Etat membre dans lequel le fournisseur de services numérique concerné a son principal établissement dans l'Union, ce qui correspond en principe à l'endroit où il a son siège social dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard. Ce critère ne devrait pas dépendre du fait de savoir si les réseaux et systèmes d'information sont physiquement situés dans un lieu donné ; la présence et l'utilisation de tels systèmes ne constituent pas en soi l'établissement principal et ne sont donc pas des critères permettant de déterminer l'établissement principal ».
http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L1148&from=FR

ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

54 Dans la Convention de Budapest, le terme de « fournisseur de services »[40] est utilisé au sens large, comme le définit l'article 1c :

> c « fournisseur de services » désigne :
> i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
> ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

55 L'article 18 de la Convention de Budapest est un important outil pour traiter certains problèmes de l'informatique dans le cloud. Si, au titre de l'article 18.1.a, il est possible pour les autorités compétentes de la Partie d'enjoindre à toute personne morale ou physique de produire tout type de données, l'article 18.1.b se limite aux fournisseurs de service « offrant des prestations sur le territoire de la Partie », qui doivent communiquer uniquement les données relatives aux abonnés.

56 Le Rapport explicatif (paragraphe 173) de la Convention de Budapest indique que le lieu réel où se trouvent les données n'est pas pertinent :

> En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction.

57 Ce même Rapport (paragraphe 171) indique par ailleurs que l'injonction de produire visée à l'article 18 peut aussi être utile lorsqu'un fournisseur de services souhaite coopérer volontairement avec les services répressifs :

> Une « injonction de produire » constitue une mesure souple que les services répressifs peuvent mettre en œuvre dans bien des situations, en particulier dans les cas où il n'est pas nécessaire de recourir à une mesure plus contraignante ou plus onéreuse. L'instauration d'un

[40] Contrairement aux outils actuels de l'UE, qui distinguent les fournisseurs de services de communications électroniques et les fournisseurs de services de la société d'information. Cette distinction est remise en question dans le contexte de la réforme de la Directive vie privée et communications électroniques : https://ec.europa.eu/digital-single-market/en/news/eprivacy-Directive-commission-launches-public-consultation-kick-start-review (en anglais)

> tel mécanisme procédural sera aussi utile pour les tiers gardiens des données qui, tels les fournisseurs d'accès Internet, sont souvent disposés à collaborer avec les services de lutte contre la criminalité sur une base volontaire en leur fournissant les données sous leur contrôle, mais préfèrent disposer d'une base juridique appropriée pour apporter cette aide, les déchargeant de toute responsabilité contractuelle ou autre.

58 Concernant l'article 18.1.b et la production des données relatives aux abonnés par un fournisseur de services offrant des prestations sur le territoire d'une Partie, le Groupe de travail sur les preuves dans le cloud a examiné la jurisprudence de la Cour de justice de l'Union européenne, en particulier les affaires en lien avec « l'offre d'un service à » ou « l'acheminement d'un service vers » un État membre de l'Union européenne, notamment les affaires C-131/12 (Google Spain), C-230/14 (Weltimmo)[41], C-595/08 et C-144/09 (Pammer et Halpenof).

59 Dans l'affaire relative à la protection des données Google Spain c. Costeja, la Cour de justice de l'Union européenne a examiné la question de l'application territoriale de la Directive 95/46 de l'UE et a déclaré ce qui suit :

> « L'article 4, paragraphe 1, sous a), de la Directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un Etat membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un Etat membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet Etat membre[42] ».

60 Dans les affaires de droit civil Pammer et Halpenof, la Cour de justice de l'Union européenne, examinant la question de savoir « si un commerçant, dont l'activité est présentée sur son site Internet ou sur celui d'un intermédiaire, peut être considéré comme « dirigeant » son activité vers l'Etat membre sur le territoire duquel le consommateur a son domicile, au sens de l'article 15, paragraphe 1, sous c) du règlement nº 44/2001 », a estimé ce qui suit :

> il convient de vérifier si, avant la conclusion éventuelle d'un contrat avec le consommateur, il ressort de ces sites Internet et de l'activité globale du commerçant que ce dernier envisageait de commercer avec des consommateurs domiciliés dans un ou plusieurs Etats membres, dont celui dans lequel ce consommateur a son domicile, en ce sens qu'il était disposé à conclure un contrat avec eux.
>
> Les éléments suivants, dont la liste n'est pas exhaustive, sont susceptibles de constituer des indices permettant de considérer que l'activité du commerçant est dirigée vers l'Etat membre du domicile du consommateur, à savoir la nature internationale de l'activité, la mention d'itinéraires à partir d'autres Etats membres pour se rendre au lieu où le commerçant est établi, l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'Etat membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue, la mention de coordonnées téléphoniques avec l'indication d'un préfixe international, l'engagement de dépenses dans un service de référencement sur Internet afin de faciliter aux consommateurs domiciliés dans d'autres Etats membres l'accès au site du commerçant ou à celui de son

[41] Arrêt rendu le 1er octobre 2015
http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=222584
Plateforme web en langue hongroise
– Les consommateurs mettent des annonces en ligne pour des biens immobiliers situés en Hongrie
– Les serveurs sont situés en Allemagne
– La plateforme appartient à une entité slovaque, qui n'a aucune activité en Slovaquie et qui n'est pas présente en Hongrie, mais qui y possède un compte bancaire, une boîte postale et un représentant chargé de résoudre les litiges.
Question : Weltimmo est-elle soumise aux lois de Hongrie ?

[42] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR

> intermédiaire, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'Etat membre où le commerçant est établi et la mention d'une clientèle internationale composée de clients domiciliés dans différents Etats membres. Il appartient au juge national de vérifier l'existence de tels indices.
> En revanche, la simple accessibilité du site Internet du commerçant ou de celui de l'intermédiaire dans l'Etat membre sur le territoire duquel le consommateur est domicilié est insuffisante. Il en va de même de la mention d'une adresse électronique ainsi que d'autres coordonnées ou de l'emploi d'une langue ou d'une monnaie qui sont la langue et/ou la monnaie habituellement utilisées dans l'Etat membre dans lequel le commerçant est établi[43].

61 Dans l'affaire Weltimmo (C-230/14)[44] portant sur la protection des données, la Cour de justice de l'Union européenne a souligné le fait que la définition du terme « établissement » doit être souple :

> 28 S'agissant, en premier lieu, de la notion d'« établissement », il convient de rappeler que le considérant 19 de la Directive 95/46 énonce que l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable et que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante (arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 48). Ce considérant précise, par ailleurs, que, lorsqu'un même responsable est établi sur le territoire de plusieurs Etats membres, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit applicable aux activités de chacun d'eux.
> 29 Il en découle, ainsi que l'a relevé en substance M. l'avocat général aux points 28 et 32 à 34 de ses conclusions, une conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée. Ainsi, afin de déterminer si une société, responsable d'un traitement de données, dispose d'un établissement, au sens de la Directive 95/46, dans un État membre autre que l'Etat membre ou le pays tiers où elle est immatriculée, il convient d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans cet autre Etat membre, en tenant compte de la nature spécifique des activités économiques et des prestations de services en question. Cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet.
> 30 A cet égard, il y a lieu, notamment, de considérer, au vu de l'objectif poursuivi par cette Directive, consistant à assurer une protection efficace et complète du droit à la vie privée et à éviter tout contournement, que la présence d'un seul représentant peut, dans certaines circonstances, suffire pour constituer une installation stable si celui-ci agit avec un degré de stabilité suffisant à l'aide des moyens nécessaires à la fourniture des services concrets concernés, dans l'Etat membre en question.
> 31 En outre, afin de réaliser ledit objectif, il y a lieu de considérer que la notion d'« établissement », au sens de la Directive 95/46, s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable.

62 Le Groupe de travail sur les preuves dans le cloud a noté avec intérêt les dispositions juridiques des Philippines qui définissent le fait de « mener des activités » dans la section 1 de la loi républicaine 5455[45] comme suit :

---

[43] Arrêt rendu le 7 décembre 2010. http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-585/08

[44] http://curia.europa.eu/juris/document/document_print.jsf?doclang=Fr&text=&pageIndex=0&part=1&mode=lst&docid=168944&occ=first&dir=&cid=21880

[45] Intitulée *Loi visant notamment à exiger que les investissements et la poursuite d'une activité commerciale sur le territoire des Philippines par des ressortissants étrangers, ou par des entités commerciales possédées intégralement ou en partie par des ressortissants étrangers, contribuent en toute indépendance à l'équilibre et à la solidité de l'économie nationale*. Approuvée le 30 septembre 1968.

> l'expression « mener une activité commerciale » désigne le fait de passer des commandes, d'effectuer des achats, de conclure des contrats de services ou d'ouvrir des succursales (qu'il s'agisse de bureaux de liaison ou de filiales) ; de désigner des représentants ou des revendeurs domiciliés dans les Philippines ou étant présents aux Philippines, pour une ou plusieurs périodes représentant un total minimal de cent huit jours pendant quelque année calendaire que ce soit ; de participer à la gestion, à la supervision ou au contrôle de toute entreprise, entité ou corporation basée aux Philippines, et tout autre acte impliquant des opérations commerciales ou arrangements commerciaux dans la continuité, et inclut donc la réalisation d'actes ou d'opérations, ou l'exercice de certaines des fonctions normalement liées à l'obtention de bénéfices commerciaux, ou à la poursuite progressive de tels bénéfices, ou de l'objectif et de la finalité de l'entreprise.

63 Le Groupe de travail sur les preuves dans le cloud a également étudié l'affaire de la Belgique contre Yahoo! dans laquelle la Cour suprême de Belgique a rendu un arrêt le 1er décembre 2015[46], résumé ci-après :

> Dans son arrêt du 1er décembre 2015, la Cour suprême de Belgique a décidé que l'entreprise Yahoo! Inc., immatriculée en Californie (Etats-Unis), était tenue de communiquer les données relatives aux abonnés et qu'elle devait donc se soumettre à la mesure coercitive de l'article 46 bis du Code d'instruction criminelle belge.
>
> Yahoo! Inc. avait fait appel d'une décision de la Cour d'appel d'Anvers du 20 novembre 2013 en avançant, entre autres raisons, que la loi coutumière internationale interdisait à un Etat d'appliquer de manière extraterritoriale les compétences qui lui incombaient.
>
> La Cour suprême de Belgique a décidé ce qui suit :
>
> - L'article 46 bis, paragraphe 2 du Code d'instruction criminelle est effectivement une mesure coercitive. Le refus d'obtempérer est passible d'une amende.
> - De manière générale, un Etat ne peut appliquer des mesures coercitives que sur son territoire, sous peine de porter atteinte à la souveraineté d'un autre pays.
> - « Un Etat impose une mesure coercitive sur son propre territoire dès lors qu'il existe, entre cette mesure et ce territoire, un lien territorial suffisant ».
> - L'article 46 bis, paragraphe 2 du Code d'instruction criminelle belge « a pour seul but le respect par les opérateurs et les fournisseurs de services ayant une activité en Belgique d'une mesure visant à obtenir uniquement des données d'identification en cas d'infraction, lorsque l'enquête correspondante relève de la compétence des services répressifs belges. Cette mesure n'exige pas la présence à l'étranger des forces de police ou des magistrats belges ou de leurs représentants, ni aucune action ou opération matérielle à l'étranger. Cette mesure a donc une portée limitée, et son exécution ne nécessite aucune intervention hors du territoire belge. »
> - Yahoo! Inc., « en tant que fournisseur de services de messagerie gratuit, est présent sur le territoire belge et se soumet à la loi belge sur une base volontaire, puisque l'entreprise participe activement à la vie économique belge, en utilisant le nom de domaine « yahoo.be » et la langue du pays, en diffusant des publicités en lien avec le lieu où se trouvent les utilisateurs de ses services et en permettant à ses utilisateurs belges de le contacter au moyen d'une boîte aux lettres et d'un service d'assistance en Belgique ».

[46] http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1 (en néerlandais)

- « la demande du ministère public n'est pas adressée à un citoyen américain sur le territoire des Etats-Unis, mais à un citoyen américain offrant des services sur le territoire belge ».
- Il n'est, de ce fait, pas question d'exercice d'un pouvoir de juridiction extraterritorial.

64 Cette décision confirme qu'une injonction faite à un fournisseur offrant ses services sur le territoire d'une Partie (et étant donc « présent » sur ce territoire) de produire des données relatives aux abonnés est une ordonnance nationale (tout comme l'article 18.1.b) et non une question de coopération internationale ou l'exercice d'une compétence extraterritoriale.

65 Le Groupe de travail sur les preuves dans le cloud a examiné d'autres affaires, parmi lesquelles Microsoft c. United States, qui porte sur un mandat de perquisition d'un compte de messagerie électronique contrôlé et géré par Microsoft sur un serveur situé en Irlande. Dans une décision rendue en juillet 2016, une Cour d'appel des Etats-Unis a estimé que le gouvernement des Etats-Unis ne peut pas contraindre une entreprise à transmettre les courriers électroniques de ses clients conservés sur des serveurs situés hors du territoire des Etats-Unis[47]. La Cour a conclu que « le Congrès n'a pas donné aux dispositions de la loi sur les communications stockées (Stored Communications Act) une application extraterritoriale » et qu'« un mandat au titre de la loi sur les communications stockées ne peut s'appliquer qu'aux données stockées sur le territoire des Etats-Unis ». Cette décision met en avant les limites d'une loi nationale particulière, mais présente néanmoins certains points intéressants.

66 La décision renvoie à la notion de « courtoisie »[48] :

> Aujourd'hui, nos conclusions servent également les intérêts de la courtoisie qui, comme les traités d'entraide le montrent, régit habituellement la conduite des enquêtes pénales transnationales. Il est vrai que nous ne pouvons connaître avec certitude la portée des obligations auxquelles les lois d'un Etat souverain étranger (et, en particulier ici, l'Irlande et l'Union européenne) contraignent un fournisseur de services qui stocke des données numériques ou qui mène des activités commerciales sur le territoire de celle-ci. Il est cependant difficile de rejeter d'emblée ces intérêts en avançant la théorie qu'aucune atteinte n'est portée aux intérêts de l'Etat souverain étranger lorsqu'un juge des Etats-Unis ordonne à un fournisseur de services de « collecter » sur des serveurs situés à l'étranger et d'« importer » vers les Etats-Unis des données pouvant appartenir à un ressortissant étranger, simplement parce que le fournisseur de services mène ses opérations depuis le territoire des Etats-Unis.
>
> C'est pourquoi, la mise en œuvre du mandat, dans la mesure où celui-ci contraint Microsoft à saisir le contenu des communications de ces clients stocké en Irlande, constitue une application extraterritoriale et illégale de la loi [49].

[47] http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412 (en anglais)

[48] Les conclusions de la Cour suprême des Etats-Unis dans l'affaire Hilton c. Guyot (1895) selon lesquelles l'application d'un arrêt délivré par un tribunal étranger relève de la courtoisie, sont une référence en droit international.[14][15] Dans cette affaire, le tribunal a conclu ce qui suit : « La « courtoisie », au sens juridique, n'est pas une obligation absolue ni une question de bonne volonté. Il s'agit de la reconnaissance offerte par une nation sur son territoire des actes législatifs, exécutifs ou judiciaires d'une autre nation, en tenant dûment compte de ses devoirs à l'international et de la convenance, ainsi que des droits de ses propres ressortissants ou d'autres personnes placées sous la protection de ses lois.

[49] Page 42 : http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412

67 Le juge Gerard Lynch, marquant son accord avec cette décision, a insisté sur « la nécessité pour le Congrès de réviser une loi désuète[50] ». Il a notamment fait les observations suivantes :

> Parce que Microsoft s'appuie uniquement sur les informations données par ses clients pour les classer selon leur lieu de résidence, que l'entreprise stocke les messages électroniques (seulement la plus grande partie, et uniquement pour des questions d'efficacité et de qualité du service clients) sur des serveurs locaux, et que le gouvernement n'a pas précisé cette information dans sa demande de mandats, comme il l'avait fait pour la cible de l'enquête, nous ne connaissons pas la nationalité du client. Si celui-ci est Irlandais (ce qui semble être le cas), cette affaire pourrait avoir d'inquiétantes retombées sur le plan international : les griefs du Gouvernement irlandais et de l'Union européenne pourraient en effet être nombreux si les Etats-Unis cherchaient à obtenir les messages électroniques d'un ressortissant irlandais, stockés en Irlande, auprès d'une entreprise américaine offrant ses services à des clients irlandais en Irlande. L'affaire n'est pas tout à fait semblable, du moins c'est ce que je crois, et j'espère que les citoyens et les autorités de l'Irlande et de l'UE le pensent aussi ; [il en ira différemment] si le gouvernement américain demande à une entreprise américaine de lui remettre les messages électroniques d'un ressortissant américain résidant aux Etats-Unis, lesquels sont accessibles d'un simple clic depuis Redmond (État de Washington), mais sont stockés sur un serveur en Irlande simplement parce que le ressortissant américain n'a pas indiqué son lieu de résidence réel dans le but de contourner la loi américaine pour mieux lui porter atteinte sur le territoire des Etats-Unis, en exploitant la politique de l'entreprise américaine qui a été mise en place uniquement pour des raisons de convenance et qui pourrait être modifiée, de manière générale ou dans sa façon d'être appliquée à ce client en particulier, selon le bon vouloir de l'entreprise américaine.
>
> Etant donné qu'une demande d'extraterritorialité est nécessaire pour saisir la volonté du Congrès, il me semble qu'il serait pour le moins formaliste de considérer cette requête comme une demande d'exercice extraterritorial d'un pouvoir alors qu'il s'agit en fait du pouvoir d'assignation d'un tribunal américain.

68 Concernant la divulgation aux autorités étrangères des données relatives aux abonnés et au trafic par les fournisseurs de services, telle qu'elle est autorisée par la loi sur le caractère privé des communications électroniques, et également des données relatives au contenu, des options, actuellement en discussion entre les États-Unis et le Royaume-Uni, pourraient permettre aux fournisseurs de services de répondre aux requêtes soumises légalement par des autorités étrangères. En juillet 2016, le ministère de la Justice des Etats-Unis a envoyé une proposition législative au Congrès relative à la divulgation des données relatives au contenu par les fournisseurs de services dans le cadre d'une procédure légale dans le pays étranger si celle-ci porte sur des communications entre ressortissants étrangers à l'étranger et des activités criminelles menées hors du territoire des Etats-Unis, sans qu'il y ait de lien avec les Etats-Unis autre que le fait que les données soient stockées sur leur territoire[51]. La divulgation devrait respecter les droits de l'homme dans le pays qui en fait la demande[52].

69 A l'heure actuelle, la pratique et les procédures, tout comme les conditions et les garanties de l'accès aux données relatives aux abonnés prévues par la loi nationale, varient considérablement selon les Parties à la Convention[53].

[50] Déclaration du ministère de la Justice dans un courrier adressé au Congrès et datée du 15 juillet 2016
[51] https://assets.documentcloud.org/documents/2994379/2016-7-15-US-UK-Biden-With-Enclosures.pdf (en anglais)
[52] Dans la lettre explicative, le ministère de la Justice déclare qu'il prévoit d'envoyer des propositions supplémentaires pour aborder les problèmes apparus dans le cadre de l'affaire du mandat de perquisition de Microsoft.
[53] En octobre 2015, le Groupe de travail sur les preuves dans le cloud a envoyé un questionnaire aux Parties et aux observateurs portant sur l'application de l'article 18.1.b (voir la compilation des réponses reçues dans le document T-CY(2015)22) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a0873 (en anglais)

70 Le Groupe de travail sur les preuves dans le cloud est d'avis qu'établir un régime distinct pour l'accès aux données relatives aux abonnés conformément à l'article 18 contribuera de manière significative à améliorer l'efficacité de la procédure d'entraide judiciaire en matière de cybercriminalité et de preuves électroniques. Une Note d'orientation sur l'article 18 et les données relatives aux abonnés, représentant l'interprétation générale qu'en font les Parties, est nécessaire. Elle pourrait aider à « 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 », comme le recommandait déjà le T-CY en décembre 2014[54]. Ainsi, il serait possible de recourir de manière plus claire à l'article 18 en tant que fondement juridique des demandes directes aux fournisseurs de services dans d'autres juridictions proposant des prestations sur le territoire d'une Partie.

## 3.5 « Divulgation volontaire » par des entités du secteur privé aux autorités judiciaires dans les juridictions étrangères

71 Certains fournisseurs peuvent répondre de manière directe à des demandes légales de données relatives aux abonnés et au trafic soumises par des autorités judiciaires dans d'autres juridictions où ils offrent leurs services. Ils peuvent également conserver des données si ces autorités leur en font la demande directement. La divulgation volontaire est une pratique majoritairement employée par les fournisseurs de services américains, car elle est prévue par la loi sur le caractère privé des communications électroniques.

72 Le Groupe de travail sur les preuves dans le cloud a organisé deux rencontres avec les fournisseurs de services en 2015 et 2016, et a élaboré un document de réflexion[55].

73 Celui-ci montre que la coopération transnationale avec les fournisseurs de services américains est pratiquée par presque toutes les Parties à la Convention de Budapest, même si toutes n'y ont pas recours de la même façon. Par exemple, en 2014, plus de 100 000 requêtes ont été envoyées par des Parties à la Convention (autres que les Etats-Unis) à l'attention de six fournisseurs de premier plan, et ont obtenu un taux de réponse de 60 % environ. En 2015, le nombre de demandes a dépassé les 138 000, avec un taux de réponse identique.

| Demandes directes de données et divulgation volontaire en 2015 | Demandes à Apple, Facebook, Google, Microsoft, Twitter et Yahoo[56] | | |
|---|---|---|---|
| Parties | Reçues | Divulgation | % |
| Albanie | 13 | 11 | 85 % |
| Arménie | 13 | 10 | 77 % |
| Australie | 6 777 | 4 580 | 68 % |
| Autriche | 254 | 119 | 47 % |
| Azerbaïdjan | 5 | - | 0 % |
| Belgique | 1 992 | 1 453 | 73 % |
| Bosnie-Herzégovine | 26 | 8 | 31 % |
| Bulgarie | 8 | 2 | 25 % |

[54] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044e292
[55] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651f04
[56] Source : rapports sur la transparence (en anglais)
Apple http://www.apple.com/privacy/transparency-reports/
Facebook https://govtrequests.facebook.com/about/#
Google https://www.google.com/transparencyreport/
Microsoft https://www.microsoft.com/about/csr/transparencyhub/
Twitter https://transparency.twitter.com/
Yahoo https://transparency.yahoo.com/government-data-requests

| Demandes directes de données et divulgation volontaire en 2015 | Demandes à Apple, Facebook, Google, Microsoft, Twitter et Yahoo[56] | | |
|---|---|---|---|
| Parties | Reçues | Divulgation | % |
| Canada | 1 157 | 884 | 76 % |
| Croatie | 33 | 19 | 58 % |
| Chypre | 24 | 4 | 17 % |
| République Tchèque | 431 | 261 | 61 % |
| Danemark | 342 | 166 | 49 % |
| République dominicaine | 207 | 114 | 55 % |
| Estonie | 79 | 52 | 66 % |
| Finlande | 227 | 172 | 76 % |
| France | 27 213 | 14 746 | 54 % |
| Géorgie | 4 | 3 | 75 % |
| Allemagne | 29 092 | 15 469 | 53 % |
| Hongrie | 584 | 214 | 37 % |
| Islande | 3 | 2 | 67 % |
| Italie | 7 847 | 3 591 | 46 % |
| Japon | 2 018 | 1 112 | 55 % |
| Lettonie | - | - | |
| Lichtenstein | 7 | 3 | 43 % |
| Lituanie | 158 | 87 | 55 % |
| Luxembourg | 122 | 83 | 68 % |
| Malte | 628 | 338 | 54 % |
| Maurice | - | - | |
| Moldova | 15 | 6 | 40 % |
| Monténégro | 21 | 10 | 48 % |
| Pays-Bas | 1 605 | 1 213 | 76 % |
| Norvège | 373 | 234 | 63 % |
| Panama | 5 | 3 | 60 % |
| Pologne | 2 378 | 820 | 34 % |
| Portugal | 3 255 | 1 751 | 54 % |
| Roumanie | 76 | 30 | 39 % |
| Serbie | 60 | 41 | 68 % |
| Slovaquie | 102 | 29 | 28 % |
| Slovénie | 22 | 14 | 64% |
| Espagne | 4 151 | 2 092 | 50 % |
| Sri Lanka | 2 | 1 | 50 % |
| Suisse | 534 | 267 | 50 % |
| « ex-République yougoslave de Macédoine » | 33 | 17 | 52 % |
| Turquie | 16 760 | 11 418 | 68 % |
| Ukraine | 19 | 5 | 26 % |
| Royaume-Uni | 29 937 | 21 075 | 70 % |
| Etats-Unis | 89 350 | 70 116 | 78 % |
| Total sans les Etats-Unis | 138 612 | 82 529 | 60 % |
| Total avec les Etats-Unis | 227 962 | 152 644 | 67 % |

74 L'étude met en avant l'importance de cette coopération, en particulier venant des fournisseurs américains :

- la Cour européenne des droits de l'homme, dans l'affaire K.U. c. Finlande[57] en décembre 2008, a confirmé l'obligation des Etats de protéger les droits de la personne, notamment par l'intermédiaire de mesures pénales efficaces. Dans son analyse, la Cour a fait référence aux dispositions relatives au droit pénal dans la Convention de Budapest, plus particulièrement en ce qui concerne la communication des données relatives aux abonnés, conformément à l'article 18. La Cour a également fait référence à la nécessaire efficacité de la coopération entre les fournisseurs de services et les autorités judiciaires, comme cela est expliqué dans les orientations adoptées par la Conférence Octopus du Conseil de l'Europe en avril 2008[58].

- Par conséquent, la coopération entre les fournisseurs de services et les services répressifs est nécessaire pour la prévention des infractions et la justice pénale, pour le renforcement de la prééminence du droit et pour la protection des droits de l'homme.

- Aux Etats-Unis, les fournisseurs de services coopèrent souvent directement avec les services répressifs des autres Parties à la Convention de Budapest et divulguent couramment les données relatives aux abonnés. Le Groupe de travail sur les preuves dans le cloud estime que, d'une certaine manière, cette pratique est conforme à l'esprit de l'article 18.1.b de la Convention de Budapest.

- Dans ce contexte, un fournisseur de services qui possède ou qui exerce un contrôle sur les données coopère avec des services répressifs ayant compétence pour traiter une infraction spécifique qui fait l'objet d'une enquête. Le lieu où se trouvent les données et les serveurs importe peu.

- Les Parties à la Convention de Budapest (autres que les États-Unis) soumettent plus de 135 000 demandes chaque année à des fournisseurs de services américains de premier plan et reçoivent des données (au moins partielles) dans environ 60 % des cas.

75 Si cette pratique des fournisseurs de services américains est plus importante dans le cadre de la prévention des infractions et de la justice pénale, le Groupe de travail sur les preuves dans le cloud formule plusieurs observations fondées sur l'étude mentionnée plus haut et sur les rencontres avec des fournisseurs et des autorités de protection des données :

- le caractère évolutif des politiques appliquées par le fournisseur et le manque de prévisibilité de la divulgation :
  Les politiques appliquées par les fournisseurs sont évolutives et imprévisibles pour les services répressifs et pour les clients. Les fournisseurs peuvent les modifier unilatéralement, à tout moment et sans que les services répressifs en soient informés au préalable.
  En outre, les politiques et les pratiques varient grandement d'un fournisseur à l'autre et d'une Partie à la Convention de Budapest à l'autre. Il est possible qu'un premier fournisseur réponde à plusieurs demandes émanant d'un pays, mais à aucune ou à quelques-unes uniquement des demandes soumises par un autre, et qu'un deuxième fasse exactement le contraire.

[57] http://hudoc.echr.coe.int/eng#{"dmdocnumber":["843777"],"itemid":["001-89964"]} (en anglais)
[58] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba (en anglais)

Etant donné le caractère volontaire de la coopération, la décision finale de divulgation des données appartient au fournisseur de services, avec possibilité de recours.
Dans l'ensemble, les politiques et les pratiques des fournisseurs sont évolutives et imprévisibles, ce qui s'avère problématique lorsqu'il est question de la prééminence du droit.

- Différence entre les fournisseurs aux Etats-Unis et les fournisseurs « européens » et autres :
  Les fournisseurs implantés aux Etats-Unis peuvent divulguer aux services répressifs étrangers les données relatives aux abonnés et au trafic, sans intermédiaire, dans le cadre d'une demande conforme à la législation des Etats-Unis (et plus particulièrement à la loi relative au caractère privé des communications électroniques)[59] ; ce n'est pas le cas des fournisseurs européens. La cause en est généralement la législation nationale (relative notamment à la conservation des données et la vie privée en ligne) qui précise que les données doivent être communiquées uniquement aux autorités de poursuite nationales dans le respect d'une procédure officielle[60].
  Par conséquent, on constate l'existence d'un flux unidirectionnel de données communiquées par les fournisseurs de services implantés aux États-Unis aux services répressifs d'Europe et d'autres régions, alors que les fournisseurs de services d'Europe ou d'autres Parties ne divulguent pas les données directement et volontairement aux autorités des Etats-Unis ou d'autres Parties.
  Les fournisseurs de services basés aux Etats-Unis sont de mieux en mieux représentés dans l'Union européenne, notamment par l'intermédiaire de filiales en Irlande, et sont donc soumis à la loi européenne, en particulier pour ce qui est de la réglementation en matière de protection des données, ce qui pourrait à l'avenir compromettre la coopération transnationale volontaire.
  En outre, au sein de l'Union européenne, la distinction est faite entre les fournisseurs de services qui proposent des services de communications électroniques (actuellement soumis aux exigences de confidentialité de la Directive vie privée et communications électroniques)[61] et les fournisseurs d'accès à Internet[62].

- Lieu où se trouvent les données :
  Pour la plupart des fournisseurs implantés aux Etats-Unis, le lieu où se trouvent les données relatives aux abonnés semble être d'une pertinence limitée.
  Les conditions d'accès aux données relatives aux abonnés semblent être déterminées par (a) le lieu où est implanté le fournisseur de services et les règles auxquelles il doit se soumettre, et (b) la compétence du service répressif demandeur relative à l'infraction faisant l'objet d'une enquête. Dans certaines conditions, les fournisseurs de services aux Etats-Unis divulguent les données relatives aux abonnés aux services répressifs dans les pays où ils offrent leurs services, comme le prévoit l'article 18.1.b de la Convention de Budapest. Cependant, plusieurs fournisseurs de premier plan ont des règles qui leur sont propres et qui excluent la divulgation de données lorsque l'adresse IP renvoie vers un pays autre que le pays demandeur.

[59] Code des Etats-Unis, titre 18, paragraphe 2702 : https://www.law.cornell.edu/uscode/text/18/2702 (en anglais)
[60] Par exemple, en Italie, les plus importants fournisseurs de télécommunications d'Italie (Tim, Vodafone, Wind et H3G) ont reçu seulement quatre demandes de données soumises directement par les services répressifs d'Europe. Ils ont répondu qu'une demande d'entraide judiciaire présentée au titre d'un accord entre Etat devait être soumise à l'autorité pénale nationale compétente, conformément à la loi italienne sur la protection des données (décret législatif nº 196 du 30 juin 2003 – Code de protection des données à caractère personnel, section 132).
http://www.garanteprivacy.it/home_en/italian-legislation (en anglais)
[61] Cette Directive (2002/58/CE) est en cours de révision https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-Directive (en anglais)
[62] Selon la définition dans la Directive sur le commerce électronique 2000/31/CE de 2000
http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32000L0031&from=FR

Les fournisseurs basés en Europe sont plutôt soumis au principe de la territorialité, et plus particulièrement au lieu où se trouvent les données. L'audition qui s'est tenue le 30 novembre 2015[63] laisse penser que ceci constitue pour les fournisseurs européens un obstacle majeur à la poursuite de leur activité. Pour ce qui est des données relatives au contenu, les fournisseurs américains sont peu clairs. Il arrive qu'ils fassent valoir que, le contenu étant stocké sur le territoire des Etats-Unis, une divulgation volontaire n'est pas possible (sauf en cas d'urgence). Lorsque les données sont stockées en Europe, ils peuvent malgré tout exiger qu'une demande d'entraide judiciaire soit soumise au Gouvernement des Etats-Unis.

- Protection des données :

  Plus les fournisseurs américains sont implantés en Europe, plus ils doivent se soumettre à la réglementation européenne en matière de protection des données.

  Les instruments européens et internationaux de protection des données s'appliquent aux transferts de données entre deux entités du secteur privé ou entre deux autorités judiciaires compétentes.

  Le transfert « asymétrique » de données entre les services répressifs d'une juridiction vers une entité du secteur privé d'une autre juridiction, dans un autre Etat (par exemple, lorsqu'une adresse IP est envoyée pour demander la communication des données relatives à l'abonné correspondant) est permis sous certaines conditions[64].

  Cependant, aucune réglementation ne permet clairement la divulgation volontaire « asymétrique » de données, c'est-à-dire depuis un fournisseur de services du secteur privé vers les services répressifs d'un autre État.

  Il incombe aux fournisseurs eux-mêmes de déterminer s'ils respectent les conditions légales, et s'il est dans l'intérêt du public ou dans leur propre intérêt en tant que contrôleur des données de les divulguer. Ils courent le risque de voir leur responsabilité engagée. Un cadre plus clair, précisant les conditions et les garanties de la divulgation transnationale de données d'une entité du secteur privé vers une autorité publique, est nécessaire.

- Fondement juridique national pour obtenir les données relatives aux abonnés :

  La coopération avec les fournisseurs est favorisée lorsque le fondement juridique de l'injonction de produire est clair. Comme le T-CY l'a documenté dans son rapport sur les règles concernant l'obtention de données relatives aux abonnés[65], les conditions à remplir pour accéder à ces données varient selon les Parties. Ainsi, pour certaines, ce sont les officiers de police judiciaire qui peuvent demander à obtenir ces données, quand pour d'autres ce sont les procureurs. Des ordonnances de tribunaux peuvent aussi être exigées, sans quoi les fournisseurs de services peuvent ne pas répondre à une demande émanant de la police ou d'une autorité de poursuite.

  Un cadre juridique clair pour l'obtention des données relatives aux abonnés, qui plus est harmonisé entre les Parties, favoriserait la coopération avec les fournisseurs dans les juridictions étrangères et l'utilisation de renseignements collectés lors de procédures pénales, en les rendant plus systématiques.

- Demandes de conservation directes :

[63] http://www.coe.int/en/web/cybercrime/hearing (en anglais)
[64] Article 14 de la décision-cadre 2008/977/JAI : http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008F0977&from=FR et article 39 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[65] T-CY (2014)17 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e743d

Les fournisseurs de services aux Etats-Unis répondent favorablement à toutes les demandes de conservation de données reçues directement d'autorités étrangères, car ils s'attendent à ce qu'elles soient suivies d'une demande de divulgation dans le cadre de l'entraide judiciaire. Le fait que, souvent, la procédure ne se poursuive pas sous la forme de l'entraide judiciaire est pour eux un sujet de préoccupation.
Les fournisseurs européens ne donnent pas suite aux demandes de conservation reçues directement des services répressifs des autres juridictions.

- Demandes urgentes :
  Les fournisseurs de services aux Etats-Unis définissent des procédures de coopération pour les situations d'urgence, portant notamment sur la divulgation de contenu.
  Certaines Parties ont défini des procédures particulières, notamment par l'intermédiaire de systèmes centralisés avec des points de contact. Le retour d'expérience de cette pratique semble être généralement positif, même si la coopération avec certains fournisseurs est considérée comme pouvant être imprévisible et peu fiable, même en situation d'urgence.
  Il semblerait donc que, si les fournisseurs américains ont pour principe de coopérer dans les situations d'urgence, leurs homologues européens ne divulguent pas les données relatives aux abonnés ou autres, même en situation d'urgence.

- Notification des clients :
  Les services répressifs ont mis en évidence les pratiques divergentes des fournisseurs pour ce qui est de la notification à leurs clients d'une demande portant sur « leurs » données et émanant d'une autorité étrangère. Ce point peut avoir des répercussions sur le déroulement d'une enquête pénale. Le fait que les fournisseurs américains informent leurs clients d'une demande émise par une autorité étrangère constitue une préoccupation de premier plan pour les services répressifs[66].
  Si des exigences de confidentialité peuvent être mises en place dans le cadre des demandes formulées sur le territoire national, il n'en va pas de même lorsqu'il est question de coopération volontaire avec un fournisseur étranger.

- Injonctions judiaires ou coopération volontaire :
  Une injonction émanant d'un officier de police judiciaire, d'un procureur ou d'un juge habilité à l'encontre d'une personne physique ou morale est contraignante et peut être appliquée sur le territoire de l'autorité.
  Néanmoins, on constate que, dans la pratique actuelle en matière de coopération directe transfrontalière, les fournisseurs de services établis aux Etats-Unis considèrent leur coopération comme « volontaire », et demandent régulièrement l'envoi de l'injonction exécutoire dans le pays concerné, même si elle ne le sera pas aux Etats-Unis.
  Les pratiques actuelles semblent mêler coopération volontaire et demande judiciaire et coercitive.
  Les fournisseurs de services implantés aux Etats-Unis semblent préférer conserver cette pratique plutôt qu'une autre.
  Dans le cadre de la répression, cette pratique peut poser problème, car ce sont les fournisseurs de services qui déterminent s'ils souhaitent coopérer, si la demande est légale, ou contrôlent s'il y a double incrimination, et le respect d'autres conditions. Sont concernées non seulement les demandes de données formulées par la police, mais également par les procureurs et les tribunaux et, finalement, ces demandes ne sont pas exécutoires[67]. Le fait que les fournisseurs de services aient un tel niveau de discrétion pose un problème de droit.

[66] Dans de nombreux pays, la loi définit comme confidentielles les demandes d'application de la loi. Les demandeurs de ces pays peuvent ignorer que ce n'est pas le cas aux Etats-Unis, à moins d'en avoir été informés.

76 Le Groupe de travail sur les preuves dans le cloud conclut donc ce qui suit :

- Il serait souhaitable que les politiques et les procédures opérationnelles de tous les types de fournisseurs de services soient plus cohérentes et transparentes, par exemple à l'aide de notes d'orientation ou grâce à l'autorégulation. Il est nécessaire de poursuivre le dialogue avec les fournisseurs de services. Des réunions régulières entre le T-CY et les fournisseurs de services, la mise en place d'un outil en ligne donnant la dernière version des politiques et procédures des fournisseurs et des renseignements sur la législation applicable et les autorités judiciaires compétentes dans chaque partie, et des modèles de demande de divulgation des données relatives aux abonnés peuvent améliorer les pratiques actuelles des Parties à la Convention de Budapest.

- Cependant, une amélioration des pratiques ne sera pas suffisante. Il est urgent d'établir des cadres juridiques clairs à l'échelle nationale et internationale, de manière à garantir une meilleure sécurité juridique appliquée à la répression et à l'industrie du droit, et à abattre les obstacles rencontrés par les entreprises[68]. Une telle solution peut se fonder sur l'article 18 de la Convention de Budapest et les dispositions d'un Protocole additionnel à la Convention.

## 3.6 Procédures d'urgence

77 En cas d'urgence, des procédures adaptées permettant d'obtenir, par l'intermédiaire de l'entraide judiciaire, des éléments de preuve stockés dans une juridiction étrangère afin d'éviter tout danger imminent menaçant la vie ou la sécurité publique sont nécessaires.

78 Le T-CY, dans son rapport d'évaluation sur les dispositions de la Convention de Budapest relatives à l'entraide judiciaire[69] de décembre 2014, a également adopté la Recommandation 8, selon laquelle « Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service ». Le Groupe de travail sur les preuves dans le cloud a assuré le suivi de cette question en avril et mai 2016 en invitant les Parties à répondre à un questionnaire.

79 Le Groupe de travail sur les preuves dans le cloud a remarqué que les fournisseurs de services implantés aux Etats-Unis offrent également une coopération directe en cas d'urgence, notamment pour ce qui est de la communication des données relatives au contenu[70]. Le questionnaire portait sur les demandes urgentes requérant la divulgation immédiate de données par l'intermédiaire de l'entraide judiciaire, mais également sur les demandes directement adressées aux fournisseurs de services.

80 Voici ce qui ressort des réponses de 33 Parties et Etats observateurs[71] :

[67] Voir à ce sujet l'arrêt de la Cour de cassation de Belgique confirmant l'obligation pour Yahoo! de produire des données lorsque la demande lui en est faite sur le sol belge.
http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f (en anglais)
[68] La même conclusion a été tirée après l'audience des fournisseurs de services tenue le 30 novembre 2015 :
http://www.coe.int/en/web/cybercrime/hearing (en anglais)
[69] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d
[70] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651f04
[71] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f (en anglais)

- La majorité des Etats ayant répondu au questionnaire (20 Etats, soit 61 %) n'ont pas de législation prévoyant la divulgation des données par les fournisseurs de services aux autorités judiciaires en cas d'urgence sans autorisation judiciaire.

- Parmi les 13 Etats (39 %) prévoyant l'obtention de données sur le territoire national en cas d'urgence, sept peuvent obtenir tous les types de données, cinq peuvent obtenir uniquement des données autres que celles relatives au contenu, et un Etat seulement peut recueillir les données relatives aux abonnés sans autorisation judiciaire.

- Seuls six Etats sur 33 (18 %) ont des procédures en place pour divulguer sans délai des données aux autorités étrangères. Un autre Etat a invoqué l'article 29.7 de la Convention de Budapest comme fondement de la coopération en cas d'urgence, sans que celle-ci soit prévue par sa législation.

- A l'exception de deux Etats (le Japon et les Etats-Unis), aucun ne dispose d'une législation autorisant un fournisseur de services implanté sur son territoire à divulguer des données aux services répressifs étrangères en cas d'urgence sans entraide judiciaire.

- Des fournisseurs de services de premier plan implantés aux Etats-Unis ont des procédures déjà en place régissant la divulgation des données à des autorités nationales et étrangères en cas d'urgence[72]. Ces procédures peuvent être applicables aux graves menaces à la vie et à la sécurité des individus, à la sûreté de l'Etat, aux graves dommages à des infrastructures essentielles (Apple), à l'atteinte imminente à l'intégrité physique d'un enfant ou au risque de décès ou de graves dommages corporels d'une personne (Facebook) et à la nécessité d'empêcher le décès ou les blessures graves de personnes (Google, Microsoft, Twitter et Yahoo!). La communication des données est à la discrétion du fournisseur de services. Celui-ci peut également informer le client sans délai ou sous 90 jours.

- Les fournisseurs implantés en Europe et ailleurs ne semblent pas avoir de procédures d'urgence en place ni coopérer directement avec les autorités étrangères en cas d'urgence.

81 Le Groupe de travail sur les preuves dans le cloud conclut ce qui suit :

- La Recommandation 8 du rapport d'évaluation du T-CY doit encore être mise en œuvre dans la majorité des Parties et des Etats observateurs, et le T-CY devrait encourager les Parties à le faire. Il pourra être nécessaire d'envisager l'élaboration d'une disposition particulière dans un Protocole à la Convention de Budapest de manière à garantir une plus grande cohésion entre les Parties.

- Il conviendrait d'examiner plus en détails la possibilité d'autoriser les fournisseurs de services à répondre directement aux demandes des autorités étrangères en cas d'urgence, comme cela est déjà le cas aux Etats-Unis et, dans une certaine mesure, au Japon.

- Il serait souhaitable que les procédures opérationnelles de divulgation des données en cas d'urgence par tous les types de fournisseurs de service soient plus cohérentes et transparentes.

[72] Voir pages 18 à 20 de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651f04

## 3.7 Exigences relatives à la protection des données

82 Actuellement, la majorité des Parties à la Convention de Budapest sont Parties à la Convention 108 du Conseil de l'Europe relative à la protection des données[73], et presque la moitié d'entre elles sont membres de l'Union européenne, et de ce fait soumises à la réglementation européenne sur la protection des données.

83 Au titre du nouveau Règlement général de l'UE sur la protection des données, les entreprises possédant des données relatives à des personnes concernées qui se trouvent dans l'Union européenne[74] doivent désigner des responsables du traitement dans l'Union et se soumettre aux lois de l'UE concernant la protection des données. Le cadre de l'UE a une large portée territoriale[75].

84 Les instruments européens de protection des données présentent donc un intérêt pour les États non-membres de l'UE Parties à la Convention de Budapest, puisqu'ils peuvent modifier la façon dont ils coopèrent avec les Etats membres de l'UE et les Parties à la Convention 108.

85 Parmi les instruments actuellement en vigueur, on peut citer les textes suivants :

- Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108)[76]
- Recommandation du Conseil de l'Europe « R(87)15 visant à réguler l'utilisation de données à caractère personnel dans le secteur de la police »[77]
- Directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[78]
- Décision-cadre 2008/977/JAI de l'Union européenne relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[79]
- Directive vie privée et communications électroniques (2002/58/CE)[80].

86 En mai 2016, l'Union européenne a publié à son Journal officiel les textes de deux nouveaux instruments adoptés :

- le Règlement général sur la protection des données[81], qui entrera en vigueur le 25 mai 2018 ;

[73] Outre les 47 Etats membres du Conseil de l'Europe, Maurice a adhéré en juin 2016 et l'Uruguay en avril 2013. Le Cap-vert, le Maroc, le Sénégal et la Tunisie ont été invités à adhérer (au 31 juillet 2016). http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=nopYjPBz

[74] Voir les articles 3 et 27 du futur règlement de l'UE.

[75] L'article 3 du futur Règlement général sur la protection des données et l'article 4 de la Directive en vigueur 95/46/CE précise la portée territoriale du cadre juridique applicable en matière de protection des données de l'UE. L'article 3 du Règlement général sur la protection des données prévoit que celui-ci doit s'appliquer au responsable du traitement ou du sous-traitement établi dans l'UE, même si le traitement des données s'effectue à l'extérieur de l'UE, et également au traitement des données à caractère personnel des personnes concernées se trouvant dans l'UE, même lorsque le responsable du traitement ou du sous-traitement n'est pas implanté dans l'UE, si le traitement est en lien avec l'offre de biens ou de services auxdites personnes concernées dans l'UE.

[76] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108

[77] https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2

[78] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

[79] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008F0977&from=FR

[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive vie privée et communications électroniques), amendée en 2009. La version révisée consolidée est disponible au lien suivant : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:FR:PDF

[81] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des

- la Directive relative au traitement des données par les autorités compétentes[82], qui doit être transposée par les Etats membres avant le 6 mai 2018.

87 Actuellement, le Conseil de l'Europe arrive au bout du processus de révision de sa Convention 108 sur la protection des données[83].

88 Les discussions tenues avec les organisations de protection des données[84] concernant les nouvelles normes européennes en la matière ont abouti aux conclusions suivantes :

- Le nouveau Règlement général sur la protection des données, la nouvelle Directive de l'UE et la version révisée de la Convention 108 du Conseil de l'Europe ne devraient pas remettre en question la forme actuelle de la Convention de Budapest :

  - la Convention de Budapest exige de ses Parties qu'elles mettent en place, par le biais du droit pénal et procédural, des compétences spécifiques pour les services répressifs encadrées par des conditions et des garanties. Ces compétences procédurales constituent une dérogation licite aux principes de la protection des données.
  - La Convention de Budapest et plus particulièrement ses dispositions sur la coopération internationale sont le fondement juridique du partage international des données à caractère personnel entre autorités publiques compétentes, notamment les autorités judiciaires. La procédure d'entraide judiciaire est conçue pour garantir le respect des exigences de prééminence du droit et la protection des droits de la personne, notamment si les données recherchées doivent être utilisées comme éléments de preuve lors de procédures pénales.

- Des problèmes de protection des données peuvent survenir lorsqu'une autorité de la justice pénale divulgue des données à caractère personnel à un fournisseur de services établi dans une autre juridiction dans le cadre d'une enquête criminelle. Pour que le fournisseur puisse répondre favorablement à une demande, il est nécessaire que l'autorité de justice pénale fournisse un minimum d'informations personnelles (comme le nom, l'adresse de messagerie électronique ou l'adresse IP) :

  - pour les États membres de l'UE, de telles divulgations « asymétriques » d'une autorité publique compétente vers une entité du secteur privé seront couvertes par la nouvelle Directive de l'UE sur la police. Lorsque la communication de données se fera par un fournisseur de services sur le territoire de l'UE, elle ne sera pas considérée comme un transfert international, et les principes généraux contenus dans la Directive devront être appliqués. En principe, cela ne devrait poser aucun problème. Dans la pratique, il devrait exister un

---

personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (Règlement général sur la protection des données) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

[82] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infraction pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[83] En juin 2016, le comité ad hoc sur la protection des données (CAHDATA) a terminé ses travaux sur le Protocole d'amendement et l'a transmis au Comité des Ministres. https://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2016)RAPAbr_Fr%20FINAL%2027%2006%202016.pdf http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2016)01_F.pdf

[84] http://www.coe.int/fr/web/cybercrime/exchange-of-views

fondement juridique national pour de tels transferts. La mise en œuvre de l'article 18 pourrait servir de fondement juridique, une fois les critères de la Directive de l'UE remplis.

- Lorsque la divulgation porte sur les informations minimales et qu'elle se fait d'une autorité de la justice pénale sur le territoire de l'UE vers un fournisseur dans un « pays tiers »[85], c'est le chapitre V de la Directive qui s'applique ; il prévoit que les transferts de données sont possibles conformément aux dispositions de l'article 39 intitulé « Transferts de données à caractère personnel à des destinataires établis dans des pays tiers ». L'article 39 est une dérogation au principe général contenu dans l'article 35(1)(b) selon lequel les transferts ne devraient se faire qu'entre autorités compétentes. C'est pourquoi il devrait être interprété de manière restrictive, et n'être utilisé qu'au cas par cas, dans le cadre d'enquêtes spécifiques, lorsqu'aucun autre outil de transfert ne peut être employé. Il ne doit pas servir de fondement juridique à des transferts répétés, habituels et portant sur des gros volumes de données personnelles. Cette dérogation est sans préjudice de « tout accord international bilatéral ou multilatéral en vigueur entre les États membres et des pays tiers dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière ».

  Dans ce contexte, le Groupe de travail sur les preuves dans le cloud estime ce qui suit :

  - si une demande de divulgation de données relatives aux abonnés portant sur des informations personnelles est envoyée par une autorité de la justice pénale à un fournisseur de services situé dans une autre juridiction mais offrant une prestation sur le territoire de l'autorité demandeuse, l'article 18.1.b peut servir de fondement juridique si le projet de Note d'orientation (voir en annexe) est avalisé par le T-CY.
  - Un Protocole à la Convention de Budapest pourrait prévoir d'autres conditions applicables aux demandes adressées aux fournisseurs de services dans les pays tiers et ainsi représenter un accord international au sens de l'article 39.2 de la Directive de l'UE sur le traitement des données personnelles par les autorités compétentes.

- Des problèmes de protection des données apparaissent également lorsqu'un fournisseur de services établi sur le territoire de l'Union européenne divulgue des données à caractère personnel directement à une autorité de la justice pénale d'une autre juridiction[86].

[85] Les règles de protection des données de l'UE font la distinction entre les Etats membres de l'UE, les Etats considérés comme ayant un niveau de protection adéquat et auxquels des données peuvent être transférées sans garanties supplémentaires (parmi les Parties à la Convention de Budapest, l'Islande, le Liechtenstein et la Norvège sont considérés comme ayant un niveau de protection adéquat étant donné qu'ils sont membres de la zone économique européenne ; des décisions d'adéquation ont été adoptées pour le Canada, Israël et la Suisse, et les entreprises des Etats-Unis sont considérées comme ayant le niveau de protection adéquat une fois le bouclier de protection des données UE-Etats-Unis adopté).
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (en anglais)
http://europa.eu/rapid/press-release_IP-16-2461_fr.htm
A l'heure actuelle, les décisions d'adéquation ne portent pas sur les échanges dans le domaine de la répression. Cependant, la nouvelle Directive de l'UE sur le traitement des données personnelles par les autorités compétentes (applicable dès mai 2018) s'appliquera également dans ce cadre.

[86] Dans l'échange de vues du 23 mai 2016, certains participants ont exprimé leur inquiétude concernant l'article 32 (accès transfrontalier aux données) et la question de savoir si un fournisseur de services peut accepter de communiquer des données au titre de cette disposition. Cependant, d'autres ont pointé du doigt le passage de la Note d'orientation formulé comme suit : « Il est peu probable que les prestataires de services remplissent les conditions d'un consentement valide et volontaire concernant la divulgation des données de leurs utilisateurs dans les conditions de l'article 32 ».
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7F_REV_GN3_transborder_V13.pdf

- En vertu du droit communautaire sur la protection des données, la divulgation de données personnelles par un fournisseur de services sur le territoire de l'UE à une autorité de la justice pénale d'une autre juridiction relève du Règlement général sur la protection des données[87]. Si la situation correspond à l'un des cas définis à l'article 6 du Règlement général sur la protection des données, un fournisseur de services sur le territoire de l'UE peut communiquer des données à une autorité de la justice pénale sur le territoire de l'UE si elle respecte les règles de protection des données. Dans la pratique et conformément aux règles actuelles, la divulgation de données par un fournisseur de services sur le territoire de l'UE directement à une autorité de la justice pénale dans un autre Etat membre de l'UE dépend de la mise en œuvre par l'Etat membre de la Directive 95/46/CE et de la Directive vie privée et communications électroniques[88].

- La divulgation de données à caractère personnel par un fournisseur de services sur le territoire de l'UE à une autorité de la justice pénale dans un pays tiers semble possible au moyen d'une décision d'adéquation (article 45 du Règlement général sur la protection des données), de garanties appropriées (article 46) ou de dérogations pour des situations particulières (article 49), qui sont des exceptions à l'article 44 (Interdiction générale des transferts internationaux à l'extérieur de l'UE) et sont donc soumises à une interprétation restrictive. En outre, l'article 48 sur les transferts ou divulgations non autorisés par le droit de l'Union fait référence aux accords internationaux en tant que fondement possible pour le transfert ou la divulgation de données par une autorité dans un pays tiers dans le cadre d'une demande légale.

  Dans ce contexte, le Groupe de travail sur les preuves dans le cloud estime ce qui suit :

  - si des données relatives aux abonnés sont divulguées par un fournisseur de services à une autorité de la justice pénale dans une autre juridiction dans le cadre d'une injonction de produire, l'article 18.1.b peut servir de fondement juridique si le fournisseur de services offre une prestation sur le territoire de l'autorité demandeuse, si la Note d'orientation (voir en annexe) est maintenue par le T-CY.
  - Un Protocole à la Convention de Budapest pourrait prévoir d'autres dispositions applicables à la divulgation de données relatives aux abonnés à une autorité de justice pénale dans un pays tiers.

- La pratique des fournisseurs de services implantés aux Etats-Unis qui consiste à avertir les clients des demandes légales de données est une préoccupation majeure des autorités judiciaires, car elle peut compromettre les enquêtes et mettre en danger, entre autres, les enquêteurs et les procureurs. Le fait d'informer le client n'est pas une exigence générale de la réglementation européenne en matière de protection des

[87] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR
[88] Par exemple, la communication de données aux autorités étrangères par Facebook Ireland est considérée comme compatible avec la législation irlandaise en matière de protection des données. En 2011 et 2012, Facebook Ireland a été entendu par le Commissaire pour la protection des données après la divulgation de données à des autorités étrangères.
Voir la section 3.7 (page 98ff) et l'Annexe 5 du rapport de 2011 (en anglais) :
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
Voir la section 3.7 (page 34ff) du rapport de 2012 (en anglais) :
https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm

données. Des exigences de confidentialité peuvent être imposées en droit interne, et les codes de procédure pénale de la plupart des pays européens semblent les prévoir.

# 4 Solutions

89 Le Groupe de travail sur les preuves dans le cloud, prenant en considération les travaux du Comité de la Convention sur la cybercriminalité sur l'entraide judiciaire, les données relatives aux abonnés, l'accès transfrontalier aux données et d'autres thèmes, et s'appuyant sur des faits nouveaux à l'échelle européenne et internationale, propose au T-CY un ensemble de solutions pour examen. Elles ne doivent pas être considérées comme des alternatives, mais doivent être mises en œuvre en parallèle.

## 4.1 Mesures juridiques et pratiques à l'échelle nationale pour améliorer l'efficacité de l'entraide judiciaire (recommandations 1 à 15 du rapport d'évaluation du T-CY sur l'entraide judiciaire)[89]

90 Le Groupe de travail sur les preuves dans le cloud conclut que l'entraide judiciaire reste le principal moyen d'obtenir des éléments de preuve électroniques auprès de juridictions étrangères pour les utiliser lors de procédures pénales sur le territoire national. Ceci est particulièrement vrai pour les données relatives au contenu.

91 Le Groupe de travail sur les preuves dans le cloud estime que, s'il est souvent impossible de mettre en place une entraide judiciaire dans le contexte de l'informatique dans le cloud, les possibilités qu'elle offre doivent être pleinement exploitées. Dans le cas contraire, les approches nouvelles et innovantes ne pourraient pas remporter une large adhésion.

92 Les Parties devraient donc assurer le suivi des recommandations suivantes, adoptées par le T-CY en décembre 2014, et dont la responsabilité incombe en premier lieu aux autorités nationales :

Rec 1 Les Parties devraient pleinement mettre en œuvre et appliquer les dispositions de la Convention de Budapest sur la cybercriminalité, y compris les pouvoirs en matière de conservation (suite au rapport d'évaluation de 2012 du T-CY).

Rec 2 Les Parties devraient envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficacité du processus d'entraide en ce qui concerne la cybercriminalité et les preuves électroniques.

Rec 3 Les Parties devraient envisager, pour l'entraide, d'affecter davantage de personnel et du personnel plus formé aux technologies, non seulement au niveau central mais aussi au niveau des institutions responsables de l'exécution des demandes (par exemple les Bureaux locaux des procureurs).

Rec 4 Les Parties devraient envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques. La formation et l'échange d'expériences devraient en particulier viser les procureurs et les juges et encourager une coopération directe entre autorités judiciaires. Une telle formation devrait être soutenue par les programmes de consolidation de capacités du Conseil de l'Europe et d'autres organisations.

Rec 5 Renforcer le rôle des points de contact 24/7 conformément à l'article 35 Convention de Budapest, notamment :

a. veiller, conformément à l'article 35.3 Convention de Budapest, à disposer de personnel

[89] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir des activités liées à l'entraide ;

b. veiller à ce que les points de contact promeuvent activement leur rôle auprès des autorités nationales et de leurs homologues étrangères ;
c. assurer des réunions régulières et la formation du réseau 24/7 ;
d. les autorités compétentes et les points de contact 24/7 devraient envisager des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et faire un retour d'information à l'Etat requérant ;
e. établir, dans la mesure du possible, des points de contacts (supplémentaires) dans les services de poursuite pour permettre un rôle plus direct en matière d'entraide et une réponse plus rapide aux demandes ;
f. les points de contact 24/7 devraient jouer au moins un rôle de soutien pour les demandes « Article 31 ».

Rec 6 Les Parties devraient envisager de rationaliser les procédures et réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard, les Parties devraient partager les bonnes pratiques avec le T-CY.

Rec 7 Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.

Rec 8 Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.

Rec 9 Les Parties devraient confirmer la réception des demandes systématiquement et notifier les actions prises.

Rec 10 Les Parties peuvent envisager l'ouverture d'une enquête nationale sur demande étrangère ou l'information spontanée pour faciliter le partage d'informations ou accélérer l'entraide.

Rec 11 Les Parties devraient utiliser la transmission électronique des demandes, conformément à l'article 25.3 Convention de Budapest relatif aux moyens de communication rapide.

Rec 12 Les Parties veillent à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.

Rec 13 Conformément à l'article 25.5 Convention de Budapest et au Paragraphe 259 du Rapport explicatif, les Parties sont encouragées à faire preuve de flexibilité lorsqu'elles appliquent la double incrimination qui faciliterait l'octroi de l'aide.

Rec 14 Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.

Rec 15 Les Parties devraient assurer la transparence en ce qui concerne les conditions applicables en matière de demandes d'entraide, et les raisons de refus, notamment pour les seuils concernant les affaires vénielles, sur les sites Web des autorités centrales.

93 La Recommandation 8, relative aux procédures d'urgence, devrait également apparaître dans un Protocole à la Convention de Budapest.

94 Le T-CY devrait examiner en détail le suivi des recommandations 1 à 5 assuré par les Parties.

95 Le Conseil de l'Europe, par l'intermédiaire de projets de renforcement des capacités, devrait apporter un soutien à la mise en œuvre des recommandations 1 à 15 lorsque cela s'avère nécessaire, et assurer le suivi des recommandations 17 et 18 :

Rec 17 Le Conseil de l'Europe devrait - par des projets de renforcement des capacités - élaborer ou créer des liens vers des formulaires modèles standardisés plurilingues pour les demandes de l'article 31.

Rec 18 Le Conseil de l'Europe devrait explorer la possibilité d'établir un fonds de ressources en ligne contenant des informations sur les systèmes de droit interne des Parties concernant les preuves électroniques et la cybercriminalité, ainsi que les seuils légaux, les conditions applicables aux preuves et autres qui doivent être remplis pour obtenir la communication de données informatiques stockées en vue de leur utilisation devant les tribunaux.

## 4.2 Note d'orientation sur l'article 18 de la Convention de Budapest concernant l'obtention des données relatives aux abonnés et éclaircissements concernant les critères qui font qu'un fournisseur de services se trouve dans la juridiction d'une autorité de la justice pénale

96 Le Groupe de travail sur les preuves dans le cloud recommande que le T-CY envisage d'adopter une Note d'orientation abordant la question de l'injonction de produire les données relatives aux abonnés au titre de l'article 18, dans les situations suivantes :

- lorsque la personne à qui il est ordonné de communiquer des données spécifiées est présente sur le territoire d'une Partie (article 18.1.a)[90] ;
- lorsque le fournisseur de services à qui il est ordonné de communiquer les données relatives aux abonnés offre une prestation sur le territoire de la Partie sans nécessairement y être présent (article 18.1.b).

97 Une Note d'orientation concernant ces aspects relatifs à l'article 18 est pertinente, étant donné que :

- les données relatives aux abonnés sont les données les plus couramment recherchées lors d'enquêtes pénales ;
- le pouvoir visé à l'article 18 relève du droit national ;
- la croissance de l'informatique dans le cloud et du stockage de données à distance pose un certain nombre de défis pour les autorités compétentes qui souhaitent accéder à des données informatiques particulières, notamment celles relatives aux abonnés, dans le cadre d'enquêtes et de procédures pénales ;
- à l'heure actuelle, la pratique et les procédures, ainsi que les conditions et les garanties de l'accès aux données relatives aux abonnés varient considérablement d'une Partie à l'autre ;
- il est nécessaire d'aborder les questions relatives aux préoccupations concernant le respect de la vie privée et la protection des données à caractère personnel, le fondement juridique de la compétence pour ce qui est des services offerts sur le territoire d'une

[90] Il est important de rappeler que l'article 18.1.a de la Convention de Budapest ne se limite pas aux données relatives aux abonnés, mais s'applique à toutes les catégories de données informatiques spécifiées. La Note d'orientation proposée aborde uniquement la production de données relatives aux abonnés.

Partie sans que le fournisseur y soit implanté, et l'accès aux données stockées dans une juridiction étrangère ou inconnue, ou en de multiples lieux par le biais du cloud ;

- la force exécutoire des injonctions de produire d'un pays à l'extérieur de ses frontières soulève encore d'autres problèmes.

98 Une Note d'orientation aiderait les États à mieux utiliser les injonctions de produire des données relatives aux abonnés à destination de fournisseurs de services implantés ou offrant une prestation sur leur territoire, comme prévu par l'article 18 de la Convention de Budapest. Etant donné les défis liés à l'informatique dans le cloud, une meilleure utilisation de cette disposition en ce sens serait un moyen efficace d'obtenir en toute légalité le type de données le plus souvent demandé lors des enquêtes pénales. Une compréhension commune de l'article 18 (pour ce qui est des données relatives aux abonnés) telle que proposée dans la Note d'orientation en annexe permettrait aussi de faire de l'article 18 le fondement juridique de la pratique actuelle consistant à envoyer directement aux fournisseurs établis dans une juridiction étrangère des demandes portant sur les données relatives aux abonnés.

100 Un projet de Note d'orientation est annexé au présent rapport pour examen du T-CY.

## 4.3 Réglementation et procédures nationales applicables à l'accès aux données relatives aux abonnés

101 Les Parties devraient faciliter l'accès aux données relatives aux abonnés dans leur législation nationale en faisant la distinction entre données relatives au trafic et données relatives aux abonnés, et en mettant ainsi pleinement en œuvre l'article 18 de la Convention de Budapest.

> Article 18 – Injonction de produire
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :
> a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ;
> b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
>
> 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
>
> 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
> a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
> b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
> c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

102 Un renseignement relatif à l'abonné est moins sensible du point de vue du respect de la vie privée que les données relatives au trafic ou au contenu. Les conditions d'émission d'une injonction de produire des données relatives aux abonnés devraient donc être soumises à moins de garanties que pour les autres catégories de données, et il devrait en être de même pour d'autres types de pouvoirs intrusifs.

103 Alléger le cadre juridique applicable à la communication de données relatives aux abonnés facilitera les enquêtes nationales et la coopération internationale dans le contexte de l'informatique dans le cloud.

## 4.4 Mesures pratiques visant à favoriser la coopération transfrontalière entre les fournisseurs de services et les autorités judiciaires

104 Dans l'attente de solutions à plus long terme, il serait possible de prendre des mesures pratiques peuvent être prises pour favoriser la cohésion de la coopération entre les fournisseurs de services et les autorités judiciaires, en particulier pour ce qui est de la divulgation des données relatives aux abonnés suite à une demande légale soumise dans le cadre d'une enquête pénale spécifique, mais également en cas d'urgence, et en faisant référence aux intérêts légitimes et aux conditions applicables en matière de protection des données.

105 A cet effet, le Groupe de travail sur les preuves dans le cloud propose ce qui suit :

- le T-CY devrait envisager d'organiser une rencontre annuelle avec les fournisseurs de services à la suite d'une réunion plénière du T-CY afin de promouvoir auprès de ces derniers des politiques et des procédures opérationnelles plus cohérentes et plus transparentes ;

- le Conseil de l'Europe (Secrétariat du T-CY et projets de renforcement des capacités) devrait établir et tenir à jour une base de ressources en ligne sur les politiques des fournisseurs de services et les règles de procédure des Parties applicables aux injonctions de produire des données relatives aux abonnés. Les Parties devraient veiller à ce que les informations concernant leur réglementation et leurs procédures soient exemptes d'erreurs et tenues à jour ;

- le Bureau de programme du Conseil de l'Europe sur la cybercriminalité devrait inviter les fournisseurs de services à prendre part à des projets de renforcement des capacités afin de faciliter la coopération entre ces derniers et les services répressifs et d'être en mesure de les solliciter pour assurer une formation à l'utilisation de leurs procédures ;

- le T-CY pourrait coopérer avec la Commission européenne de manière à ce que les deux organisations soient informées du travail de l'autre et à donner naissance à des synergies.

## 4.5 Protocole additionnel à la Convention de Budapest

106 Le Groupe de travail sur les preuves dans le cloud recommande d'entamer la négociation d'un Protocole additionnel à la Convention de Budapest sur la cybercriminalité afin de permettre une entraide judiciaire plus efficace, de faciliter la coopération directe avec les fournisseurs de services implantés dans d'autres juridictions si nécessaire et, dans certaines conditions et selon certaines garanties, de définir les conditions et les garanties applicables aux pratiques actuelles en matière d'accès transfrontalier aux données et de définir les exigences relatives à la protection des données.

107 Il convient de rappeler, à ce sujet, que l'Assemblée parlementaire du Conseil de l'Europe, dans sa Recommandation 2077 (2015)[91] « Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet », a invité les Parties à la Convention de Budapest à notamment étudier la faisabilité d'un Protocole additionnel concernant l'accès des autorités judiciaires aux données stockées sur des serveurs dans le cloud et l'accès transfrontalier aux données en élargissant la portée de l'article 32 de la Convention.

108 Les éléments qui suivent sont des pistes de réflexion. Leur faisabilité devra être déterminée au cours de la négociation d'un Protocole. D'autres éléments peuvent également être étudiés au cours de ce processus.

### 4.5.1 Dispositions pour une entraide judiciaire plus efficace

109 Le rapport d'évaluation sur le fonctionnement de l'entraide judiciaire[92] adopté par le T-CY en décembre 2014 contient des recommandations devant être traitées au moyen d'un Protocole à la Convention de Budapest. Ces recommandations restent valides.

#### 4.5.1.1 Un cadre simplifié pour les demandes d'entraide judiciaire portant sur des données relatives aux abonnés (Recommandation 19 du rapport d'évaluation du T-CY)

110 La Recommandation 19 du rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

> Les Parties devraient considérer de permettre - par des amendements juridiques nationaux et accord international - la divulgation rapide de l'identité et l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur.

111 L'article 18 de la Convention de Budapest prévoit qu'il incombe à chaque Partie de mettre en place des mesures pour obtenir la communication de données (article 18.1.a) par une personne présente sur le territoire ou de données relatives aux abonnés par un fournisseur de services offrant une prestation sur le territoire (18.1.b). Néanmoins, cette disposition peut ne pas être applicable ni appliquée dans certains contextes.

112 Selon l'article 31 de la Convention de Budapest relatif à l'entraide concernant l'accès aux données stockées, « la demande doit être satisfaite aussi rapidement que possible ». Néanmoins, l'article 31 ne fait pas la distinction entre les différentes catégories de données et ne propose aucun mécanisme permettant de communiquer rapidement les données.

113 Vu que les données relatives aux abonnés sont généralement nécessaires dès le commencement d'une enquête, et qu'elles sont moins sensibles du point de vue du respect de la vie privée que les

[91] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=21976&lang=FR
[92] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726d

données relatives au trafic et au contenu, un Protocole pourrait permettre de définir le cadre de l'entraide judiciaire pour répondre au plus vite aux demandes de données relatives aux abonnés.

114 Un tel cadre pourrait venir en complément de l'article 18 pour ce qui est des données relatives aux abonnés, notamment lorsqu'un fournisseur de services refuse de répondre à une injonction de produire envoyée par les autorités compétentes d'une Partie où il propose ses prestations (article 18.1.b).

#### 4.5.1.2 Injonctions de produire internationales (Recommandation 20 du rapport d'évaluation du T-CY)

115 La Recommandation 20 du rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

> Les Parties intéressées peuvent étudier la possibilité et le champ d'application d'une injonction de produire internationale à adresser directement par les autorités d'une Partie aux agents des services répressifs d'une autre Partie.

116 Le T-CY pourrait pour cela s'appuyer sur la Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale[93], une décision judiciaire devant être émise par les autorités d'un Etat membre et reconnue et exécutée par les autorités d'un autre Etat membre.

> (7) Une décision d'enquête européenne doit être émise pour faire réaliser une ou plusieurs mesures d'enquête spécifiques dans l'État exécutant la décision d'enquête européenne (ci-après dénommé «État d'exécution») en vue de recueillir des preuves. Cela comprend l'obtention de preuves qui sont déjà en possession de l'autorité d'exécution.

117 Cette Directive « établit un régime unique pour l'obtention de preuves ». Elle ne s'applique pas uniquement aux éléments de preuve électroniques. Cependant, le Conseil « Justice et affaires intérieures » de l'Union européenne, dans les « Conclusions du Conseil de l'Union européenne sur l'amélioration de la justice pénale dans le cyberespace » adoptées le 9 juin 2016[94], souligne l'importance de la décision d'enquête européenne pour garantir l'obtention d'éléments de preuve électroniques au sein de l'Union européenne. Le Conseil appelle les Etats membres de l'UE à « transposer rapidement la Directive » dans leur législation nationale. En outre :

> Il est demandé à la COMMISSION, dans l'optique d'une utilisation pleine et entière de la Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale, de continuer de suivre et de soutenir les Etats membres dans le cadre du processus de transposition de cette Directive, qui doit être achevé le 22 mai 2017.

118 Lors de l'élaboration d'un projet de Protocole à la Convention de Budapest, il serait possible d'établir s'il est faisable d'intégrer des éléments relatifs à la décision d'enquête européenne pour définir une injonction de produire internationale.

#### 4.5.1.3 Coopération directe entre les autorités judiciaires dans le cadre des demandes d'entraide judiciaire (Recommandation 21 du rapport d'évaluation du T-CY)

119 La Recommandation 21 du rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

[93] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014L0041&from=FR
[94] http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09-criminal-activities-cyberspace/

> Les Parties devraient envisager de renforcer la coopération directe entre autorités judiciaires pour ce qui concerne les demandes d'entraide.

120 Concernant les canaux et les moyens de coopération, le rapport d'évaluation du T-CY sur l'entraide judiciaire conclut :

> Concl 11: La plupart des Parties recourent à différents accords bilatéraux, régionaux et multilatéraux ou s'appuient sur le principe de la réciprocité, et des multiples autorités et canaux de coopération comme prévu dans la Convention de Budapest sur la cybercriminalité. Certains Etats, cependant, suivent une approche plus limitée et exigent que les demandes de MLA soient transmises par la voie des ministères de la Justice et seul un petit nombre accepte les demandes transmises par la voie diplomatique.
>
> Concl 12 : La possibilité d'une coopération directe avec les autorités judiciaires étrangères semble être sous-utilisée – excepté entre Etats membres de l'UE. Cette utilisation limitée de l'option d'une coopération directe semble aussi la voie choisie pour des Etats non-membres de l'UE qui sont néanmoins Parties au 2e Protocole additionnel à la Convention sur l'entraide judiciaire en matière pénale (STE 182) du Conseil de l'Europe. Il serait peut-être judicieux d'envisager des dispositions permettant la coopération directe entre Parties à la Convention de Budapest.

121 La Convention de Budapest, à son article 25.3, fait référence aux moyens techniques permettant une coopération rapide et, à son article 27.2.b, à la communication directe entre les autorités centrales désignées.

122 Néanmoins, d'autres instruments relatifs à l'entraide judiciaire prévoient la possibilité de transmettre des demandes directement d'une autorité judiciaire d'une Partie requérante à une autorité judiciaire d'une Partie requise. C'est le cas de l'article 4 du deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale (STE 182)[95] du Conseil de l'Europe ou de l'article 6 de la Convention d'entraide judiciaire en matière pénale entre les Etats membres et l'Union européenne[96].

123 Un Protocole à la Convention de Budapest pourrait intégrer une disposition semblable afin que les Parties qui ne sont pas Parties aux traités concernés puissent profiter de cette possibilité.

#### 4.5.1.4 Enquêtes conjointes et équipes communes d'enquête (Recommandation 23 du rapport d'évaluation du T-CY)

124 La Recommandation 23 du Rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

> Les Parties devraient étudier la possibilité d'enquêtes conjointes et/ou la création d'équipes d'enquête conjointes.

125 Les enquêtes conjointes ou les équipes communes d'enquête peuvent être un moyen efficace d'enquêter sur des affaires de cybercriminalité transfrontalière. Si aucune disposition de la Convention de Budapest n'aborde ce sujet, le deuxième Protocole à la Convention européenne d'entraide judiciaire en matière pénale (STE 182)[97], à son article 20, définit avec précision les équipes d'enquête conjointes. Cet article reproduit presque l'intégralité de l'article 13 de la Convention européenne d'entraide judiciaire en matière pénale.

[95] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/182
[96] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:FR:PDF
[97] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/182

126 Un Protocole à la Convention de Budapest pourrait intégrer une disposition semblable à l'article 20 de la Convention européenne d'entraide judiciaire en matière pénale afin que les Parties qui ne sont pas parties aux traités concernés puissent profiter de cette possibilité.

#### 4.5.1.5 Demandes en langue anglaise (Recommandation 24 du rapport d'évaluation du T-CY)

127 La Recommandation 24 du Rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

> Les Parties devraient envisager de permettre que les demandes soient envoyées en anglais, en particulier les demandes de conservation.

128 Le Rapport d'évaluation du T-CY sur l'entraide judiciaire a souligné ce qui suit :

> La question de la langue de rédaction des demandes d'entraide internationale est, pour la plupart des Etats, un problème majeur, essentiellement du fait :
>
> - des retards induits par les traductions ;
> - du coût des traductions ;
> - de leur qualité limitée, notamment une terminologie peu claire ;
> - de la maîtrise limitée de langues étrangères par les praticiens.
>
> Même si, à des fins internes (motifs juridiques et pratiques), des traductions certifiées resteraient nécessaires, la plupart des Etats acceptent une demande rédigée en anglais.
> (...)
> Un Protocole additionnel à la Convention de Budapest pourrait prévoir que les demandes d'entraide judiciaire envoyées en anglais sont acceptées par les Partis, du moins en cas d'urgence.

129 Certaines Parties n'acceptent pas les demandes formulées en anglais, sauf si elles y sont contraintes par un accord international auquel elles sont parties. Toutefois, la Convention de Budapest ne précise pas la langue dans laquelle une demande doit être soumise.

130 Une disposition prévoyant la possibilité de soumettre une demande en anglais pourrait être intégrée à un Protocole à la Convention de Budapest, du moins pour ce qui est des demandes de conservation des données et des demandes portant sur les données relatives aux abonnés.

#### 4.5.1.6 Auditions par vidéoconférence/conférence téléphonique des témoins, victimes et experts

131 Les affaires de cybercriminalité et autres affaires impliquant des éléments de preuve électroniques font généralement intervenir des victimes et des témoins, notamment des experts, situés dans de multiples juridictions, ce qui pose d'importants obstacles pour les procédures pénales.

132 C'est pourquoi un certain nombre d'instruments internationaux prévoient la possibilité que les auditions se déroulent par vidéoconférence ou par conférence téléphonique. C'est le cas des articles 9 et 10 du deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale du Conseil de l'Europe (STE 182)[98].

[98] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/182

133 Un Protocole à la Convention de Budapest pourrait intégrer une disposition semblable aux articles 9 et 10 de la Convention européenne d'entraide judiciaire en matière pénale, afin que les Parties qui ne sont pas Parties à cet accord puissent profiter de cette possibilité.

#### 4.5.1.7 Procédures d'urgence (Recommandation 8 du rapport d'évaluation du T-CY)

134 La Recommandation 8 du rapport d'évaluation du T-CY sur l'entraide judiciaire est formulée comme suit :

> Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.

135 Selon le rapport, cette recommandation relève « de la responsabilité des autorités nationales ».

136 Une étude menée par le Groupe de travail sur les preuves dans le cloud[99] au printemps 2016, à laquelle 33 États ont participé, a conclu que :

- la législation actuelle de la majorité des Parties ne prévoit pas la communication de données aux autorités nationales de la justice pénale en cas d'urgence ;
- moins de 20 % des Parties disposent de procédures qui permettent à leurs autorités compétentes de communiquer rapidement des données à des autorités étrangères ;
- seules deux Parties ont autorisé les fournisseurs de services implantés sur leur territoire à communiquer des données à des autorités étrangères en cas d'urgence.

137 Au vu de ce qui précède et afin de garantir la cohérence des échanges entre les Parties, le Groupe de travail sur les preuves dans le cloud propose de transposer la Recommandation 8 par un Protocole à la Convention de Budapest.

### 4.5.2 Dispositions permettant la coopération directe avec les fournisseurs de services d'autres juridictions

138 Le Groupe de travail sur les preuves dans le cloud estime que l'article 18 de la Convention de Budapest, tel qu'il est expliqué dans la version provisoire de la Note d'orientation, permet d'envoyer des injonctions de produire des données relatives aux abonnés à des fournisseurs de services offrant des prestations sur le territoire d'une Partie tout en étant implantés sur le territoire d'une autre. La transposition de l'article 18 dans le droit national devrait permettre de considérer les données reçues des fournisseurs de services comme des preuves lors de procédures pénales.

139 Un Protocole à la Convention de Budapest pourrait :

- apporter des clarifications sur les procédures et les conditions de la coopération directe avec les fournisseurs de services d'autres juridictions, et sur la recevabilité des données communiquées dans le cadre d'enquêtes pénales ;

99 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f (en anglais)

- établir un fondement juridique pour les demandes directes de conservation des données adressées aux fournisseurs de services. Il s'agit d'une pratique déjà acceptée par les fournisseurs de services établis aux Etats-Unis ;

- définir des procédures d'urgence permettant la coopération directe avec les fournisseurs de services de juridictions étrangères lorsque la situation l'exige.

### 4.5.3 Un cadre plus clair et des garanties renforcées pour les pratiques actuelles en matière d'accès transfrontalier aux données[100]

140 Les options et les recommandations proposées dans le présent rapport ont pour objectif d'améliorer l'efficacité de la coopération entre les autorités judiciaires et avec les fournisseurs de services.

141 Elles n'abordent pas les différentes situations de « disparition (de la connaissance) du lieu »[101] impliquant de multiples fournisseurs et juridictions ou dans lesquelles l'origine d'une attaque est inconnue ou impossible à déterminer.

142 Entre 2012 et 2014, le Groupe du T-CY sur l'accès transfrontalier a déterminé que les instruments internationaux, en particulier l'article 32b, n'offrent que des possibilités limitées. En l'absence d'un cadre juridique international clair et concret, il est de plus en plus courant de voir les gouvernements mettre en œuvre des solutions unilatérales, avec les risques que cela peut entraîner pour les relations entre Etats et les droits de la personne[102].

143 Le Groupe sur l'accès transfrontalier a proposé une série d'options supplémentaires pouvant être intégrées à un Protocole à la Convention de Budapest. Cependant, en décembre 2014, il a conclu que :

- dans le contexte d'alors, la négociation d'un Protocole sur l'accès transfrontalier aux données n'était pas réalisable ;

- les problèmes identifiés vont se multiplier et non disparaître ;

- en l'absence d'un cadre international ayant fait l'objet d'un accord et contenant des garanties, de plus en plus de pays vont agir de manière unilatérale et étendre leurs pouvoirs répressifs aux recherches transfrontalières à distance, que ce soit de manière officielle ou non, avec des protections peu claires. Ce type de revendications unilatérales ou « sauvages » de juridiction ne constituera pas une solution satisfaisante.

144 Le Groupe de travail sur les preuves dans le cloud recommande que certaines des propositions formulées soient à nouveau examinées au moment des négociations relatives au Protocole à la Convention de Budapest[103] :

---

[100] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6 (en anglais)

[101] Voir par exemple Sansom, Gareth (2008) à propos du problème du « lieu » dans le cyberespace. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/Gareth%20Samson%20Website%20Location.pdf (en anglais)

[102] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726f

[103] En 2015, l'Assemblée parlementaire du Conseil de l'Europe a adopté la Recommandation 2077 (2015) sur « Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet », qui recommande d'élargir la portée de l'article 32 de la Convention de Budapest à l'aide d'un Protocole additionnel. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=21976&lang=FR
En réponse, le Comité des ministres du Conseil de l'Europe a formulé la remarque suivante : « Le T-CY a décidé d'être attentif à la suite des événements et [de] réexaminer à l'avenir la faisabilité d'un Protocole consacré à la question spécifique de l'accès transfrontalier aux données », et assuré que « Le Comité des Ministres a l'intention de suivre la question de près et tiendra l'Assemblée informée des développements en la matière ».

- L'accès transfrontalier sans consentement, mais par des moyens obtenus légalement. Une telle disposition pourrait permettre à une Partie de se passer de l'autorisation d'une autre Partie pour accéder, via un système informatique se trouvant sur son territoire, à des données stockées sur un système informatique situé dans une autre Partie ou pour recevoir ces données dans le cadre d'une enquête criminelle ou d'un procès pénal, à condition que les éléments obtenus l'aient été grâce à des activités d'investigation légales. La Partie menant l'enquête serait dans l'obligation d'en informer l'autre Partie avant, pendant ou après l'acquisition des données. Il serait nécessaire de définir des conditions et des garanties supplémentaires[104].

- L'accès transfrontalier sans consentement, de bonne foi ou dans des situations urgentes ou exceptionnelles. Une telle provision permettrait d'autoriser l'accès transfrontalier dans des cas spécifiques, de manière à prévenir un danger imminent, une blessure physique, l'évasion d'un suspect ou autre cas semblable. Le risque de destruction de preuves pertinentes peut constituer l'un de ces cas. Là aussi, il serait nécessaire de définir des critères et des garanties spécifiques et tenir l'autre Partie informée. La « bonne foi » devrait également être définie, lorsque, au cours d'une enquête, une autorité répressive peut ne pas être sûre ou ignorer que le système informatique recherché se trouve sur le sol d'un autre pays, ou ne pas savoir sur quel territoire il se trouve, ou encore avoir obtenu des éléments de preuve sur le territoire d'un autre pays par erreur ou par accident. Il serait nécessaire de définir des conditions et des garanties spécifiques.

- Le « pouvoir d'utilisation » ou le « responsable du traitement ou du sous-traitement » comme critère de légalité des recherches[105]. En cas de « disparition (de la connaissance) du lieu », lorsque les données sont « quelque part dans le cloud », qu'elles se déplacent d'un serveur et d'un lieu à l'autre, qu'elles sont réparties en plusieurs lieux ou composées de plusieurs sous-ensembles dynamiques de données issues de différents lieux, ou qu'elles sont en miroir ou cachées, et donc disponibles à de multiples endroits au même moment, ou lorsqu'une personne utilise l'itinérance, alors que les données sont consultées ou interceptées, il est problématique d'invoquer le principe de territorialité pour déterminer la juridiction à même d'ordonner une perquisition ou une saisie de preuves électroniques. C'est pourquoi il a été avancé qu'il serait nécessaire d'adopter une approche allant plus loin que le principe de territorialité. Le « pouvoir d'utilisation » ou le « responsable du traitement ou du sous-traitement » pourrait être un critère permettant de faire le lien pour la légalité des recherches. Même si le lieu où se trouvent les données ne peut pas être déterminé avec certitude, les données peuvent être reliées à une personne qui a la capacité d'« altérer, d'effacer, de supprimer ou de rendre inutilisables, et la capacité d'empêcher autrui d'accéder [aux données] ou de les utiliser, de quelque manière que ce soit »[106]. Il conviendrait de définir des conditions et des garanties spécifiques.

---

[104] Par exemple, il est possible de limiter cette possibilité aux cas où les informations d'identification ont été obtenues en toute légalité par les services répressifs de la Partie menant une enquête, de manière à éviter le « piratage » par les autorités des systèmes informatiques situés sur le territoire d'une autre Partie.

[105] Spoenle, Jan (2010): L'informatique dans le cloud et enquêtes sur la cybercriminalité : principe de territorialité contre pouvoir d'utilisation ("cloud computing and cybercrime investigations: territoriality vs the power of disposal"), document de réflexion, Projet sur la cybercriminalité, Conseil de l'Europe, Strasbourg. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (en anglais)
Voir également Sansom, Gareth (2008) à propos du problème du « lieu » dans le cyberespace. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/Gareth%20Samson%20Website%20Location.pdf (en anglais)

[106] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (en anglais)

### 4.5.4 Garanties, dont les exigences de protection des données

145 Il se peut que certaines des mesures proposées pour un traitement dans un Protocole à la Convention de Budapest exigent de définir des conditions et des garanties particulières, notamment des dispositions relatives à la protection des données personnelles.

146 On peut s'inspirer des accords opérationnels conclus entre EUROPOL et certains pays non membres de l'UE[107], qui portent généralement sur :

- la limitation de la finalité ;
- la nécessité de transmettre les données à caractère personnel ;
- les restrictions applicables aux transmissions ultérieures ;
- le droit d'accéder aux données ;
- la qualité des données et l'évaluation de la source et des informations ;
- le stockage, la révision, la rectification et la suppression des données à caractère personnel ;
- la sécurité des données.

147 Concernant la coopération directe entre les autorités judiciaires d'une Partie et un fournisseur de services établi dans une autre juridiction, un Protocole pourrait être nécessaire pour définir des conditions propres au transfert de données :

- d'une autorité de la justice pénale vers une entité du secteur privé établie dans une autre juridiction[108] ;
- d'une entité du secteur privé vers une autorité de la justice pénale située dans une autre juridiction.

[107] https://www.europol.europa.eu/content/page/external-cooperation-31 (en anglais)
[108] Voir l'article 39 de la Directive (UE) 2016/680 du Parlement européenne et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=EN

# 5 Recommandations au T-CY

148 Le Groupe de travail sur les preuves dans le cloud estime que la combinaison des solutions proposées constitue une réponse applicable à certains des défis de l'informatique dans le cloud auxquels doivent faire face les autorités judiciaires. C'est pourquoi il soumet au T-CY les recommandations suivantes :

Rec 1 Inviter les Parties et les Etats observateurs à assurer le suivi des Recommandations du T-CY concernant l'entraide judiciaire adoptées en décembre 2014 et relevant principalement de la responsabilité des autorités nationales, c'est-à-dire les recommandations 1 à 15[109]. Le T-CY devrait par ailleurs évaluer les progrès réalisés et les programmes de renforcement des capacités, si besoin est, afin d'apporter un appui à la mise en œuvre.

Rec 2 Examiner le projet de Note d'orientation sur les injonctions de produire des données relatives aux abonnés, telle qu'annexée au présent rapport, en vue de son adoption et pour proposer aux Parties des conseils pour la mise en œuvre de l'article 18.

Rec 3 Inviter les Parties et les Etats observateurs à évaluer leurs procédures internes concernant l'accès aux données relatives aux abonnés, et garantir ainsi la pleine mise en œuvre de l'article 18 de la Convention de Budapest.

Rec 4 Prendre des mesures pratiques (en attendant des solutions à plus long terme) pour favoriser une coopération plus cohérente entre fournisseurs de services et autorités judiciaires, particulièrement pour ce qui est de la divulgation des données relatives aux abonnés suite à une demande légale dans le cadre d'une enquête pénale ou en cas d'urgence.

Rec 5 Envisager la préparation d'un projet de Protocole à la Convention de Budapest qui contiendra :

- des dispositions pour une entraide judiciaire plus efficace :
  - simplification du régime de demande d'entraide judiciaire portant sur les données relatives aux abonnés ;
  - injonctions de produire internationales ;
  - coopération directe entre autorités judiciaires dans le cadre de l'entraide judiciaire ;
  - enquêtes conjointes et équipes communes d'enquête ;
  - formulation des demandes en anglais ;
  - audition des témoins, victimes et experts par vidéoconférence et par conférence téléphonique ;
  - procédures d'entraide judiciaire d'urgence ;

- des dispositions permettant la coopération directe avec des fournisseurs de services d'autres juridictions pour ce qui est des demandes de données relatives aux abonnés, des demandes de conservation et des demandes urgentes ;

- un cadre plus clair et des garanties renforcées appliqués aux pratiques actuelles en matière d'accès transfrontalier aux données ;

[109] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

- des garanties, notamment des exigences en matière de protection des données.

Afin de faciliter une décision officielle du T-CY avant juin 2017 concernant l'élaboration d'un projet de Protocole, le T-CY pourrait envisager d'élargir le mandat du Groupe de travail sur les preuves dans le cloud et demander à ce dernier de lui soumettre un projet de Termes de référence pour le processus de rédaction et des renseignements complémentaires sur de possibles éléments au printemps 2017.

# 6 Annexes

## 6.1 Mandat du "groupe sur les preuves dans le nuage"

| | |
|---|---|
| Nom | Groupe de travail sur l'accès de la justice pénale aux preuves stockées dans le "nuage", y compris par le biais de l'entraide judiciaire ("groupe sur les preuves dans le nuage ") |
| Origine | Le Groupe de travail du T-CY dans le cadre de l'article 1.1.j des Règles de procédure[110] établi par la décision du T-CY [adoptée lors de la 12e Réunion Plénière (2-3 décembre 2014)] |
| Durée | 1 janvier 2015 – 31 décembre 2016 |
| Objectif principal | Explorer des solutions sur l'accès de la justice pénale aux preuves stockées sur les serveurs dans les nuages et dans les juridictions étrangères notamment par le biais de l'entraide judiciaire.<br><br>Le groupe de travail prépare un rapport pour examen par le T-CY, prenant en compte :<br><br>▪ les recommandations du T-CY du rapport sur d'évaluation sur les dispositions de l'entraide judiciaire de la Convention de Budapest sur la cybercriminalité (document T-CY (2013) 17rev) ;<br><br>▪ les travaux du groupe ad hoc sur l'accès transfrontalier aux données et sur les questions de compétence territoriale ;<br><br>▪ une description détaillée de la situation actuelle et des problèmes ainsi que les défis émergents concernant l'accès de la justice pénale aux données dans le nuage et dans les juridictions étrangères.<br><br>Le rapport doit contenir des propositions d'options et des recommandations pour des d'actions futures par T-CY. |
| Indicateurs et elements livrables | ▪ Juin 2015 : document de travail avec une description des défis actuels et émergents qui servira de base pour un échange de vues avec les fournisseurs de services et d'autres intervenants à la Conférence Octopus 2015.<br>▪ Juin 2015: atelier à la Conférence Octopus.<br>▪ Décembre 2015 : rapport intérimaire aux fins d'examen par le T-CY.<br>▪ Juin 2016: projet de rapport pour examen par la T-CY.<br>▪ Décembre 2016: Rapport Final pour examen par le T-CY |
| Méthode de travail | Le groupe de travail doit se réunir immédiatement après les réunions du Bureau T-CY et à huis clos.<br><br>Le groupe de travail peut tenir des audiences publiques, publier des résultats provisoires et consulter d'autres parties concernées. |
| Composition | • Les membres du Bureau membres participe d'office avec prise en |

[110] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/t-cy(2013)F25rev_%20rules_v15.pdf

| | |
|---|---|
| | charge des frais [111]<br>• Jusqu'à5 membres supplémentaires avec prise en charge des frais[112]<br>• Membres additionnels du T-CY (Etats parties) à leur propre frais. |

[111] Soumis à la disponibilité de financement.
[112] Soumis à la disponibilité de financement.

## 6.2 Note d'orientation provisoire sur l'injonctions de production concernant des informations sur les abonnés (Article 18 Budapest Convention)

www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

T-CY(2015)16

Strasbourg, version 15 septembre 2016

Comité de la Convention de la Cybercriminalité (T-CY)

# Note d'orientation T-CY #10 (PROJET)

## Injonctions de production concernant des informations sur les abonnés (Article 18 Budapest Convention)

Proposition révisée établie par le Bureau du T – CY et le Groupe sur les Preuves dans le Cloud

**Pour commentaires des États Parties et Observateurs d'ici le 21 octobre 2016**

(conformément à la T-CY 14 : Décision concernant le point 7 -

« Inviter le Groupe sur les Preuves dans le Cloud à diffuser une version révisée de la Note d'orientation, incluant une compilation des commentaires reçus, aux États Parties et Observateurs d'ici fin septembre 2016 en vue de recueillir des commentaires supplémentaires d'ici le 21 octobre 2016 »)

Contact

Alexander Seger
Secrétaire du Comité de la Convention Cybercriminalité (T-CY)
Direction Générale des Droits de l'Homme et de l'État de droit
Conseil de l'Europe, Strasbourg, France

Tél +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

## Introduction

A sa 8e Plénière (décembre 2012), le Comité de la Convention sur la Cybercriminalité (T-CY) a décidé de publier des Notes d'orientation visant à faciliter l'usage et la mise en œuvre effectives de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des développements du droit, des politiques et des techniques[113].

Les Notes d'orientation reflètent une analyse de l'application de la Convention partagée par toutes ses Parties.

La présente Note[114] traite la question des injonctions de produire relatives à des informations sur les abonnés visées à l'article 18, à savoir dans des situations où :

une personne à qui il est fait injonction de produire des données informatiques spécifiées est présente sur le territoire d'un État Partie (Article 18.1.a) ;[115]
un fournisseur de services à qui il est fait injonction de produire des informations sur un abonné propose un service sur le territoire de l'État Partie sans forcément être situé sur le territoire en question (Article 18.1.b).

Il est pertinent de publier une Note d'orientation sur ces aspects de l'Article 18, étant donné :

que des informations sur des abonnés sont le plus souvent recherchées dans des enquêtes pénales ;
que l'article 18 a une compétence nationale ;
que, du fait de l'essor du « cloud computing » et du stockage de données à distance, les autorités compétentes cherchant à accéder à des données informatiques spécifiées - en particulier à des informations relatives à l'abonné – pour mener des enquêtes pénales et des poursuites se sont heurtées à un certain nombre de difficultés ;
qu'actuellement, les pratiques et les procédures, ainsi que les conditions et les sauvegardes en matière d'accès à des informations concernant les abonnés varient considérablement d'un État Partie de la Convention à l'autre ;
qu'il est nécessaire de traiter les problèmes qui se posent en matière de vie privée et de protection des données à caractère personnel, pour ce qui est du fondement juridique de la juridiction relative aux services offerts sur le territoire d'un État partie sans que le fournisseur de services soit établi sur ce territoire, ainsi qu'en ce qui concerne l'accès à des données stockées dans des juridictions étrangères ou en des lieux inconnus ou multiples « dans le cloud » ;
que la possibilité de faire exécuter des injonctions de produire nationales à l'encontre de fournisseurs établis hors du territoire d'un État Partie pose d'autres problèmes.

La mesure visée à l'article 18 doit s'appliquer dans des enquêtes et procédures pénales spécifiques relevant du champ d'application de l'article 14 de la Convention de Budapest. Les injonctions doivent donc être délivrées dans des cas spécifiques en ce qui concerne des abonnés spécifiés.

[113] Voir le mandat du T-CY (article 46 de la Convention de Budapest).
[114] Cette Note d'orientation s'appuie sur les travaux du Groupe sur les Preuves dans le Cloud.
[115] Il est important de rappeler que l'article 18.1.a de la Convention de Budapest n'est pas limité aux seules informations relatives aux abonnés, mais qu'il concerne tout type de données informatiques spécifiées. En revanche, la présente Note d'orientation ne traite que la seule production d'informations concernant les abonnés.

## ▪ Article 18 de la Convention de Budapest[116]

### o Texte de la disposition

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession ou sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique ; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sons son contrôle relatives aux abonnés et concernant de tels services.

Extrait du Rapport explicatif :

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé en possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, droit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Dans certains États, la notion juridique de « possession » recouvre la possession matérielle et de droit de manière assez large pour satisfaire à cette exigence de « possession ou de contrôle ».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement ou à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction[117].

[116] Voir l'annexe pour l'article 18 et les extraits *in extenso* du Rapport explicatif.
[117] Paragraphe 173 du Rapport explicatif.

### o Que recouvre l'expression « données relatives aux abonnés » ?

L'expression « données relatives aux abonnés » est définie à l'article 18.3 de la Convention de Budapest :

> 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
>
> a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
>
> b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
>
> c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

L'obtention de données relatives aux abonnés constitue une ingérence moins contraignante à l'égard des droits individuels que l'obtention de données relatives au trafic ou au contenu.

### o Qu'est-ce qu'un « fournisseur de services » ?

La Convention de Budapest sur la cybercriminalité prévoit une notion large du « fournisseur de services », qui est défini à l'article 1.c de la Convention de Budapest :

Aux fins de la présente Convention, l'expression :

> c. « fournisseur de services » désigne :
>
> i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
>
> ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

L'article 18.1.b s'applique pour tout fournisseur de services présent sur le territoire de la partie ou offrant des services sur ce dernier[118].

## ▪ Interprétation par le T-CY de l'article 18 de la Convention de Budapest en ce qui concerne les données relatives aux abonnés

### o Portée de l'article 18.1.a

La portée est large : une « personne » (notion qui peut englober celle de « fournisseur de services) physiquement ou légalement présente sur le territoire de la Partie.

Pour ce qui est des données informatiques, la portée est large mais n'est pas indéfinie : toutes données informatiques « spécifiées » (ce qui entraîne que l'article 18.1.a

[118] Les instruments de l'Union européenne font la distinction entre fournisseurs de services de communication électroniques et fournisseurs de services dans la société de l'Internet. La notion de « fournisseur de services » visée à l'article 1.c de la Convention de Budapest recouvre ces deux aspects.

n'est pas limité aux « données relatives aux abonnés » et couvre tout type de données informatiques).

Les données informatiques spécifiées sont en possession ou sous le contrôle de cette personne.

Les données informatiques spécifiées sont stockées dans un système informatique ou un moyen de stockage informatique.

L'injonction de produire est émise et exécutable par les autorités compétentes dans la Partie dans la juridiction de laquelle l'injonction est demandée/accordée.

### o Portée de l'article 18.1.b

La portée de l'article 18.1.b est plus étroite que celle de l'article 18.1.a. L'alinéa b :

est limité au « fournisseur de services »[119] ;

est limité aux « données relatives aux abonnés » ;

le fournisseur de services destinataire de l'injonction n'est pas nécessairement présent physiquement sur le territoire, mais les services sont prêtés sur le territoire et le fournisseur de services peut donc être considéré comme établi sur le territoire.

### o Compétence

L'article 18.1.b est limité aux circonstances où l'autorité de justice pénale délivrant l'injonction de produire est compétente pour l'infraction en vertu de l'article 22 de la Convention de Budapest[120].

Seront en général concernées les situations où l'abonné est ou était résident ou présent sur le territoire lors de la commission de l'infraction.

La présente interprétation de l'article 18 ne préjuge pas de compétences plus larges ou supplémentaires en vertu du droit interne des Parties.

### o Quelles sont les caractéristiques d'une « injonction de produire » ?

[119] Le concept de « personne » est plus large que celui de « fournisseur de services », même si un « fournisseur de services » peut être une « personne ».

[120] Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 – 11 de la présente Convention, lorsque l'infraction est commise :
   a sur son territoire ; ou
   b à bord d'un navire battant pavillon de cette Partie ; ou
   c à bord d'un aéronef immatriculé dans cette Partie ; ou
   d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnées à l'article 24, paragraphe 1 de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est le mieux à même d'exercer les poursuites.

Une « injonction de produire » au sens de l'article 18 est une mesure nationale qui doit être prise selon le droit pénal interne. Elle est limitée par la compétence d'adjudication et d'exécution de la Partie dans laquelle l'injonction est délivrée.

Les injections de produire relevant de l'article 18 portent « sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services. »[121]

Selon le paragraphe 171 du rapport explicatif de la Convention de Budapest, les injonctions de produire constituent une mesure souple qui est moins contraignante que la perquisition ou la saisie ou encre d'autres pouvoirs coercitifs et qui peuvent servir de base juridique appropriée pour la coopération avec les fournisseurs de services.

### o Quel effet produit la localisation des données ?

Le fait que les informations relatives aux abonnés soient stockées dans une autre juridiction ne fait pas obstacle à l'application de l'article 18 de la Convention de Budapest. Le Rapport explicatif précise :

concernant l'article 18.1.a, que « l'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication. »[122] ;

concernant l'article 18.1.b, que « l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société) »[123].

Ceci couvre les situations dans lesquelles la facilité de stockage est située hors du territoire de la Partie.

En ce qui concerne l'article 18.1.b, une des situations courantes est celle où un fournisseur de services a son siège dans une juridiction, applique le régime juridique d'une deuxième juridiction et stocke les données dans une troisième. Des données peuvent être répliquées dans plusieurs juridictions ou se déplacer entre plusieurs juridictions à la discrétion du fournisseur de services sans information ni contrôle de l'abonné. Les régimes juridiques admettent de plus en plus, tant dans la sphère du droit pénal qu'en matière de protection de la vie privée et des données, que la localisation des données n'est pas le facteur déterminant pour établir la compétence juridictionnelle.

[121] Paragraphe 172 du Rapport explicatif.
[122] Paragraphe 173 du Rapport explicatif. Une « personne » au sens de l'article 18.1.a de la Convention de Budapest peut être une personne physique ou une personne morale, notamment un fournisseur de services.
[123] Paragraphe 173 du Rapport explicatif.

### o Que recouvre la notion de « offrant des prestations sur le territoire d'une Partie » ?

L'essor du « Cloud computing » a amené à s'interroger sur le point de savoir quand un fournisseur de services est considéré comme offrant ses prestations sur le territoire de la Partie et étant par là-même tenu d'obéir à une injonction nationale de produire des données relatives à un abonné. Cette question a fait l'objet d'une série d'interprétation par les tribunaux dans diverses juridictions, dans des affaires civiles comme pénales.

Le T-CY est parvenu à la conclusion qu'en ce qui concerne l'article 18.1.b, un fournisseur de services « offre un service sur le territoire de la partie » lorsque :

le fournisseur de services permet à des personnes sur le territoire de la Partie de s'abonner à ses services (et ne bloque pas, par exemple, l'accès à ces services) ;

et

oriente ses activités vers ces abonnés (par exemple, en faisant localement de la publicité ou en faisant de la publicité dans la langue du territoire de la Partie), ou utilise les informations relatives aux abonnés (ou les données de trafic associées) dans le cours de ses activités, ou interagit avec des abonnés dans la Partie.

### o Considérations générales et sauvegardes

L'on part du principe que les Parties à la Convention forment une communauté de confiance et que les principes de l'état de droit et droits de l'homme sont respectés conformément aux dispositions de l'article 15 de la Convention de Budapest.

> Article 15.3 - Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.

### o Application de l'article 18 en ce qui concerne les données relatives aux abonnés

La production de données relatives aux abonnés en vertu de l'article 18 de la Convention de Budapest peut donc être ordonnée si les critères suivants sont remplis dans une enquête pénale spécifique et pour des abonnés spécifiés :

<table>
<tr><td colspan="3">SI<br>l'autorité de justice pénale est compétente pour l'infraction conformément à l'article 22 de la Convention de Budapest ;</td></tr>
<tr><td colspan="3">ET SI<br>le fournisseur de services possède ou contrôle les données relatives à l'abonné ;</td></tr>
<tr><td colspan="3">ET SI</td></tr>
<tr><td>Article 18.1.a<br>Le fournisseur de services est physiquement ou légalement présent ou représenté sur le territoire de la Partie. Par exemple, le fournisseur de services est enregistré en tant que fournisseur de</td><td>OU</td><td>Article 18.1.b<br>Le fournisseur de services « offre un service sur le territoire de la Partie », autrement dit :<br>- le fournisseur de services permet à des personnes sur le territoire de la Partie de s'abonner à ses services,[124] ET</td></tr>
</table>

| | | |
|---|---|---|
| services de communication électroniques, ou des serveurs ou parties de son infrastructures sont situés sur le territoire de la Partie. | | - oriente ses activités vers les abonnés, ou utilise les informations relatives aux abonnés dans le cours de ses activités, ou interagit avec des abonnés sur le territoire de la Partie ; ET<br>- les données relatives aux abonnés devant être produites concernent les services d'un fournisseur offerts sur le territoire de la Partie. |

## ▪ Déclaration du T-CY

Le T-CY s'accorde à dire que les positions présentées ci-dessus constituent le socle commun sur lequel s'entendent les Parties en ce qui concerne la portée et les éléments de l'article 18 de la Convention de Budapest concernant la production de données relatives aux abonnés.

## ▪ Annexes : Extraits de la Convention de Budapest

### Article 18 – Injonction de produire

[124] Veuillez noter le Paragraphe 183 Rapport explicatif : « La mention d'un « contrat ou arrangement de service » s'entend au sens très large de toute type de relation sur la base duquel un abonné utilise les services d'un fournisseur ».

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Rapport explicatif

170. Au paragraphe 1 de cet article, les Parties sont invitées à habiliter leurs autorités compétentes à contraindre une personne présente sur leur territoire à fournir des données informatiques stockées spécifiées ou un fournisseur de services offrant ceux-ci sur le territoire d'une Partie à communiquer les données relatives à l'abonné. Les données en question sont des données stockées ou existantes et n'englobent pas les données qui n'existent pas encore, comme les données relatives au trafic ou au contenu se rapportant aux communications futures. Au lieu de requérir des États qu'ils appliquent systématiquement des mesures contraignantes à l'égard de tiers, telles que la perquisition et la saisie de données, il est essentiel que les États disposent dans leur droit interne d'autres pouvoirs d'enquête qui leur donnent un moyen moins intrusif d'obtenir des informations utiles pour les enquêtes pénales.

171. Une « injonction de produire » constitue une mesure souple que les services répressifs peuvent mettre en oeuvre dans bien des situations, en particulier dans les cas où il n'est pas nécessaire de recourir à une mesure plus contraignante ou plus onéreuse. L'instauration d'un tel mécanisme procédural sera aussi utile pour les tiers gardiens des données qui, tels les fournisseurs d'accès Internet, sont souvent disposés à collaborer avec les services de lutte contre la criminalité sur une base volontaire en leur fournissant les données sous leur contrôle, mais préfèrent disposer d'une base juridique appropriée pour apporter cette aide, les déchargeant de toute responsabilité contractuelle ou autre.

172. L'injonction de produire porte sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services.

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, doit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Dans certains Etats, la notion juridique de « possession » recouvre la possession matérielle et de droit de manière assez large pour satisfaire à cette exigence de « possession ou de contrôle ».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction.

174. Les conditions et sauvegardes visées au paragraphe 2 de l'article peuvent, en fonction du droit interne de chaque Partie, exclure des données ou informations confidentielles. Une Partie pourra prescrire des choix différents concernant les conditions, les autorités compétentes et les sauvegardes à propos de la communication de tel ou tel type de données informatiques ou de données relatives à l'abonné détenues par telle ou telle catégorie de personnes ou de fournisseurs de services. Ainsi, par exemple, en ce qui concerne certains types de données telles que les données relatives à l'abonné connues de tous, une Partie pourra habiliter les agents de la force publique à émettre une injonction de ce genre tandis qu'une ordonnance d'un tribunal pourrait être requise dans d'autres situations. En revanche, dans certaines situations, une Partie pourrait exiger ou se voir imposer par des sauvegardes relevant des droits de l'homme d'exiger qu'une injonction de produire soit émise uniquement par une autorité judiciaire afin de pouvoir obtenir certains types de données. Les Parties pourraient souhaiter limiter la divulgation de ces données aux fins de lutte contre la criminalité aux situations dans lesquelles une injonction de produire en vue de la divulgation de ces données a été rendue par une autorité judiciaire. Par ailleurs, le principe de proportionnalité introduit une certaine souplesse dans l'application de la mesure, par exemple en l'excluant dans les affaires sans gravité.

175. Les Parties peuvent également envisager d'instaurer des mesures relatives à la confidentialité. L'article ne mentionne pas spécifiquement la confidentialité, ceci afin de préserver le parallélisme avec le monde non électronique, où la confidentialité n'est en général pas imposée en ce qui concerne les injonctions de produire. Toutefois, dans le monde électronique, et en particulier le monde en ligne, une injonction de produire peut parfois servir de mesure préliminaire dans le cadre d'une enquête, précédant d'autres mesures telles que la perquisition et la saisie ou l'interception en temps réel d'autres données. Le succès de l'enquête pourrait dépendre de la confidentialité.

176. S'agissant des modalités de production, les Parties peuvent instaurer l'obligation de produire des données informatiques ou des informations relatives à l'abonné de la manière spécifiée dans l'injonction. Elles pourraient ainsi mentionner le délai dans lequel la divulgation doit intervenir ou la forme sous laquelle les données doivent être divulguées (« texte en clair », en ligne, sortie imprimée ou disquette).

177. L'expression « informations relatives aux abonnés » est définie au paragraphe 3. En principe, elle désigne toute information détenue par l'administration d'un fournisseur de services et qui se rapporte à un abonné à ses services. Les données relatives aux abonnés peuvent être contenues sous forme de données informatiques ou sous toute autre forme, telle que des documents-papier. Comme les informations relatives aux abonnés ne se présentent pas toutes sous la forme de données informatiques, une disposition spéciale a été insérée dans l'article pour tenir compte de ce type d'informations. Le terme d'« abonné » vise à englober de nombreuses catégories de clients des fournisseurs de services : personne ayant payé un abonnement, client qui paie au fur et à mesure les services qu'il utilise, personne bénéficiant de services gratuits. Sont aussi incluses les informations concernant les personnes habilitées à utiliser le compte de l'abonné.

178. Dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires dans deux situations spécifiques. Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique.

179. En conséquence, les informations relatives aux abonnés recouvrent différents types d'informations sur l'utilisation d'un service et l'usager de ce service. S'agissant de l'utilisation du service, l'expression désigne toute information, autre que des données relatives au trafic ou au contenu, permettant d'établir le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période pendant laquelle l'intéressé a été abonné au service en question. L'expression « dispositions techniques » désigne l'ensemble des mesures prises pour permettre à l'abonné de profiter du service de communication offert.
Ces dispositions incluent notamment la réservation d'un numéro ou adresse technique (numéro de téléphone, adresse de site Web ou nom de domaine, adresse électronique, etc.) ainsi que la fourniture et l'enregistrement du matériel de communication utilisé par l'abonné (appareils de téléphonie, centres d'appel ou réseaux locaux).

180. Les informations relatives aux abonnés ne sont pas limitées aux informations se rapportant directement à l'utilisation du service de communication. Elles désignent également toutes les informations, autres que des données relatives au trafic ou au contenu, qui permettent d'établir l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'utilisateur, et tout autre numéro d'accès et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et le fournisseur de services. Elles désignent en outre toute autre information, autre que des données relatives au trafic ou au contenu, relative à l'endroit où se trouvent les équipements de communication, information disponible sur la base d'un contrat ou arrangement de service. Cette dernière information peut n'avoir d'intérêt pratique que dans le cas d'équipements non portatifs, mais le fait de savoir si les équipements en question sont portatifs ou de connaître l'endroit où ils se trouveraient (sur la base de l'information fournie en vertu du contrat ou de l'arrangement de service) peut être utile à l'enquête.

181. Cet article ne fait toutefois pas obligation aux fournisseurs de services de conserver des données sur leurs abonnés. Et les fournisseurs ne seront pas non plus tenus, en vertu de la Convention, de s'assurer de l'exactitude desdites données. En d'autres termes, les fournisseurs de services ne sont pas astreints à enregistrer les données relatives à l'identité des utilisateurs des télécartes donnant accès aux services radiotéléphoniques mobiles. Ils ne sont pas non plus obligés de vérifier l'identité des abonnés ou de s'opposer à l'emploi de pseudonymes par les utilisateurs de leurs services.

182. Les pouvoirs et procédures faisant l'objet de la présente section étant instaurés aux fins d'enquêtes ou de procédures pénales spécifiques (article 14), les injonctions de produire sont appelées à être utilisées dans des affaires individuelles concernant le plus souvent un abonné. Ainsi, par exemple, sur la base de la mention du nom de telle ou telle personne dans l'injonction de produire, un numéro de téléphone ou une adresse électronique peuvent être demandés. Sur la base d'un certain numéro de téléphone ou d'une certaine adresse électronique, le nom et l'adresse de l'abonné peuvent être demandés. La mention susvisée n'autorise pas les Parties à rendre une ordonnance aux fins de divulgation de quantités non sélectives d'informations relatives aux abonnés par un fournisseur de services relatives à des groupes d'abonnés, par exemple aux fins d'extraction de données.

183. La mention d'un « contrat ou arrangement de service » s'entend au sens très large de tout type de relation sur la base duquel un abonné utilise les services d'un fournisseur.