26 mai 2015
Strasbourg, France

T-CY (2015)10
Provisoire

Comité de la Convention cybercriminalité (T-CY)

Défis de l'accès de la justice pénale aux données stockées dans le nuage

Document de réflexion

établi par le Groupe du T-CY sur les preuves dans le nuage

www.coe.int/TCY

Table des matières

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

1 Objet du présent rapport

A sa 12e réunion plénière, les 2 et 3 décembre 2014, le comité de la Convention 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 nuage, notamment dans le cadre de l'entraide judiciaire (« Groupe sur les preuves dans le nuage » - « Cloud Evidence Group »)[1].

Cette décision a été 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[2].

Le Groupe sur les preuves dans le nuage est tenu de présenter un rapport au T-CY assorti d'options et de recommandations d'actions futures d'ici décembre 2016 (un rapport intérimaire doit être présenté d'ici décembre 2015). 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) ;
- les travaux du sous-groupe ad hoc sur l'accès transfrontalier aux données et la compétence ;
- 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 nuage et dans les juridictions étrangères.

Le présent document de réflexion a pour objet de faciliter un échange de vues sur les défis actuels et futurs auxquels doivent faire face les autorités judiciaires et de favoriser la coopération du secteur concerné et d'autres parties prenantes afin de trouver des solutions, sous forme de mesures concrètes et de documents décrivant de bonnes pratiques, mais aussi de lignes directrices ou de protocole additionnel contraignant à la Convention de Budapest sur la cybercriminalité.

Le présent rapport ne traite pas de mesures de prévention et de protection, étant entendu qu'une justice pénale effective et des mesures préventives prises à tous les niveaux sont complémentaires.

---

[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] L'Union européenne souligne également la nécessité de solutions pour permettre un accès opportun aux preuves électroniques en vue de protéger les droits des victimes (http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/fr/pdf, février 2015). Il est noté dans le programme européen en matière de sécurité (avril 2015) que : *« La cybercriminalité oblige les autorités judiciaires compétentes à repenser la manière dont elles coopèrent dans leur ressort territorial, dans le cadre légal applicable, afin d'accélérer l'accès transfrontière aux éléments de preuve et aux informations, en tenant compte des évolutions actuelles et futures des technologies, telles que l'informatique dans le cloud et l'internet des objets. La collecte de preuves électroniques en temps réel auprès d'autres États concernant, par exemple, les propriétaires d'adresses IP, et la question de leur recevabilité devant les tribunaux sont des enjeux essentiels. »*
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
Le T-CY a indiqué ce qui suit dans le document T-CY(2014)16
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf :
« Le Groupe sur l'accès transfrontalier estime qu'en l'absence d'un cadre international faisant consensus et assorti de garanties, de plus en plus de pays prendront des mesures unilatérales et étendront leurs pouvoirs répressifs aux perquisitions transfrontalières, de manière formelle ou informelle, en l'absence de garanties claires. De telles affirmations de compétence unilatérales ou intempestives ne constitueront pas une solution satisfaisante. »

Les solutions resteront dans le champ d'application de l'article 14 de la Convention de Budapest[3], c'est-à-dire qu'elles couvriront 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.

2 Menace de la cybercriminalité et problématique des preuves électroniques

2.1 Cybercriminalité et preuves électroniques

La cybercriminalité[4] et les défis que posent les preuves électroniques[5] ont atteint un niveau et une complexité tels qu'ils affectent la sécurité des technologies de l'information et de la communication (TIC) et la confiance dans ces technologies.

Il ressort d'un examen de l'ampleur, de la portée et des 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) 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, à savoir :

- le vol et l'utilisation à mauvais escient de données à caractère personnel (données de comptes de courrier électronique, données de cartes de crédit, carnets d'adresses, dossiers de patients, etc.) portent atteinte au droit à la vie privée (y compris à la protection des données à caractère personnel) de centaines de millions de personnes[6] ;
- la cybercriminalité est une atteinte à la dignité et à l'intégrité des personnes, en particulier des enfants[7] ;
- les cyberattaques (telles que les attaques par déni de service distribué, le défacement de sites web et autres types d'attaques) contre des médias, des organisations de la société civile, des personnes et des institutions publiques portent atteinte à la liberté d'expression[8] ;

[3] « 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 ; et
c à la collecte des preuves électroniques de toute infraction pénale. »

[4] Définie en l'occurrence comme l'ensemble des infractions contre et au moyen de données et de systèmes informatiques au sens des articles 2 à 11 de la Convention de Budapest sur la cybercriminalité. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[5] Les preuves électroniques de toute infraction pénale relevant des compétences de droit procédural énoncées dans la Convention de Budapest (Article 14 de la Convention de Budapest).

[6] http://www.handelsblatt.com/technik/vernetzt/russische-bande-erbeutet-nutzerdaten-was-tun-nach-dem-datendiebstahl/10297922.html
http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[7] Voir également l'arrêt de la Cour européenne des droits de l'homme dans l'affaire K.U. c. Finlande.
http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}

[8] Par exemple, les jours qui ont suivi la tragédie survenue à *Charlie Hebdo* le 7 janvier 2015, plus de 20 000 sites web ont fait l'objet de cyberattaques en France : http://www.lefigaro.fr/secteur/high-tech/2015/01/15/01007-20150115ARTFIG00333-la-france-face-a-une-vague-sans-precedent-de-cyberattaques.php
Les attaques de novembre et décembre 2014 contre Sony sont un autre exemple récent.
http://www.nbcnews.com/storyline/sony-hack/sony-hack-most-serious-cyberattack-yet-u-s-interests-clapper-n281456
http://www.bbc.com/news/entertainment-arts-30512032

- la cybercriminalité est une atteinte à la démocratie. Les gouvernements, les parlements et d'autres institutions publiques ainsi que les infrastructures critiques sont confrontés tous les jours à cette menace[9] ;
- la cybercriminalité menace la stabilité démocratique. Les technologies de l'information et de la communication sont utilisées de façon abusive pour transmettre des messages xénophobes et racistes, contribuent à la radicalisation et servent les intérêts des terroristes[10] ;
- la cybercriminalité a des répercussions économiques et présente des risques pour les sociétés, en plus de compromettre les possibilités de développement humain au moyen des TIC[11] ;
- la cybercriminalité menace la paix et la stabilité au niveau international. Les conflits militaires et les désaccords politiques s'accompagnent de plus en plus fréquemment de cyberattaques[12].

D'après les informations communiquées, les incidents mettant en cause la sécurité se comptent par milliards sur les réseaux chaque année[13] et des millions d'attaques contre des systèmes informatiques et des données sont enregistrées chaque jour[14]. La cybercriminalité est une préoccupation majeure pour les gouvernements, les sociétés et les personnes[15].

Qui plus est, les autorités judiciaires se heurtent au problème que les preuves en lien avec tout type d'infraction sont désormais souvent conservées sous forme électronique sur des systèmes informatiques[16]. Les demandes internationales de données sont liées principalement à la fraude et à d'autres délits financiers, suivis des crimes violents et des crimes graves. Cette catégorie peut couvrir le meurtre, 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[17].

Selon les prévisions, la cybercriminalité devrait prendre de l'ampleur en 2015 et au-delà, pour de multiples raisons, notamment, des vulnérabilités techniques susceptibles de toucher des centaines de millions d'utilisateurs et la sécurité d'organisations. Au nombre des exemples à retenir de 2014 figurent les menaces de malware sur des appareils mobiles[18], les failles telles que Heartbleed[19], le

[9] Voir par exemple : http://www.welt. big data and the Internet of Everything
de/politik/deutschland/article136114277/Cyber-Angriff-auf-Kanzleramt-und-Bundestag.html
[10] http://www.liberation.fr/monde/2014/09/14/la-radicalisation-des-futurs-jihadistes-est-rapide-la-plupart-sont-des-convertis_1100395
http://130.154.3.8/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
[11] Pour des liens entre la cybercriminalité et le développement humain, voir :
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercriminalité/Documents/Reports-Presentations/cyber%20CB_v1y.pdf
En dépit d'un consensus général sur l'énorme coût de la cybercriminalité, il est difficile de déterminer son coût réel et l'ampleur des dégâts occasionnés. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercriminalité2.pdf
[12] Par exemple : http://www.bbc.com/news/world-europe-30453069
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf
http://www.cbsnews.com/news/cyber-warfare-the-next-front-in-the-israel-gaza-conflict/
[13] http://www.symantec.com/deepsight-products/
[14] Voir par exemple : http://www.sicherheitstacho.eu/?lang=en
[15] http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf
[16] Par exemple, les données relatives aux abonnés ou son adresse IP concernant les mails de demande de rançon dans des affaires d'enlèvement, les données de localisation d'une personne suspectée de meurtre ou d'un trafiquant de drogue, le lien entre différents actes terroristes, etc.
[17] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf
[18] Voir l'étude conjointe de Kaspersky Lab et Interpol (octobre 2014) concernant les menaces sur les téléphones mobiles à l'adresse suivante : http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/10/report_mobile_cyberthreats_web.pdf

hacking de la norme UMTS pour les communications de téléphonie mobile[20], le clonage de données biométriques telles que les empreintes digitales[21] ou la reconnaissance de l'iris[22] ou des préoccupations liées à la sécurité des services proposés dans le nuage pour la conservation des données[23]. Les nouvelles formes de paiement électronique, y compris l'argent mobile, offrent de nouvelles possibilités de fraudes et d'autres délits financiers.

Le Big data et l'internet des objets[24] créent d'autres risques en matière de sécurité et de confidentialité, du fait de l'aspect commercial que revêt internet, de plus en plus utilisé comme source d'exploitation de données personnelles. Les données disponibles sont utilisées à des fins commerciales mais aussi parfois à des fins criminelles, sur le modèle de la récolte de données effectuée par « crime-as-a-service ».[25]

Si ne serait-ce qu'une infime partie des infractions impliquant des données et systèmes informatiques pouvaient faire l'objet de poursuites, les victimes ne seraient pas aussi désabusées par la justice. Cette situation soulève des questions quant à l'Etat de droit dans le cyberespace.

2.2 Confusion entre justice pénale et sécurité nationale

Les débats public et politique sur la surveillance massive sont marqués par une confusion entre justice pénale et sécurité nationale. Les autorités judiciaires mènent des enquêtes pénales spécifiques visant à obtenir des données précises à utiliser dans les affaires portées devant la justice et dans les procédures judiciaires. Les enquêtes pouvant interférer avec les droits des personnes, elles sont assorties de garanties relatives à l'Etat de droit[26], telles que le contrôle judiciaire, outre que les preuves peuvent être contestées et des recours sont possibles. Ce cas de figure diffère nettement de l'interception massive de données à des fins de sécurité nationale.

Malgré cela, la confusion règne. Cette situation donne lieu à des conditions supplémentaires pour les autorités judiciaires, qui empêchent de trouver des solutions pour renforcer l'efficacité des enquêtes et

---

Voir également : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-vulnerabilities-under-attack.pdf

[19] http://blogs.mcafee.com/consumer/what-is-heartbleed

[20] http://www.sueddeutsche.de/digital/mobilfunkstandard-umts-ultimativer-abhoeralbtraum-1.2281898
http://www.sueddeutsche.de/digital/abhoeren-von-handys-so-laesst-sich-das-umts-netz-knacken-1.2273436-2

[21] http://www.bbc.com/news/technology-30623611
http://www.macrumors.com/2014/12/29/ccc-reproduce-fingerprints-public-photos/

[22] http://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html

[23] http://www.denverpost.com/breakingnews/ci_26452892/apple-says-some-celebrity-accounts-compromised
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf
http://arxiv.org/pdf/1404.2697v1.pdf

[24] http://www.ft.com/cms/s/0/685fe610-9ba6-11e4-950f-00144feabdc0.html#axzz3QULEgVl1
http://drivingsalesnews.com/bmw-companies-want-our-driver-data/

[25] http://gadgets.ndtv.com/internet/news/europes-police-need-data-law-changes-to-fight-cybercrime-europol-599960
http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

[26] Voir l'article 15 de la Convention de Budapest. D'après la Cour européenne des droits de l'homme, pour être compatible avec la Convention européenne des droits de l'homme, une ingérence doit satisfaire aux conditions suivantes :

- être prévue par la loi, qui doit répondre à des conditions de précision, de clarté, d'accessibilité et de prévisibilité ;
- viser un but légitime ;
- être nécessaire, c'est-à-dire répondre à un besoin social urgent dans une société démocratique, et de fait, proportionnée ;
- autoriser des recours effectifs ;
- être soumise à des garanties contre les risques d'abus.

des poursuites dans les affaires de cybercriminalité et pour d'autres infractions impliquant des preuves électroniques[27].

Comme l'a déclaré la Secrétaire Générale adjointe du Conseil de l'Europe en mars 2015 :

> « Ce dont nous avons besoin, c'est d'une justice pénale plus efficace et de garanties renforcées concernant les mesures de sécurité nationale, et non pas d'une confusion entre les deux types d'activités qui nous empêchera de trouver des solutions au plan de la justice pénale »[28].

2.3 Incertitude quant à la disponibilité des données

Les rapports sur la surveillance massive et l'arrêt de la Cour européenne de justice concernant la directive de l'UE sur la conservation des données[29] ont suscité des incertitudes quant aux règles sur les compétences procédurales au sein de l'Union européenne mais aussi partout ailleurs. Dans certains pays, les dispositions relatives à la conservation des données ainsi que d'autres compétences permettant d'obtenir des preuves électroniques ont été supprimées ou sont remises en cause. Les retards dans l'adoption de cadres européens de protection des données au niveau de l'Union européenne et du Conseil de l'Europe ne font qu'ajouter à l'incertitude.

De plus, la coopération avec la justice pénale des prestataires de services dans le nuage et dans d'autres secteurs dépend souvent de ces prestataires, qui peuvent modifier leurs politiques internes unilatéralement à tout moment.

2.4 Types de données nécessaires à des fins pénales

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

- les données relatives aux abonnés ;
- les données relatives au trafic ;
- les données relatives au contenu.

Dans de nombreuses juridictions, les conditions d'accès aux données relatives aux abonnés sont généralement moins strictes que pour l'accès aux données relatives au trafic, tandis que le régime le plus strict s'applique aux données relatives au contenu.

2.4.1 Données relatives aux abonnés[30]

Les données relatives aux abonnés sont essentielles pour identifier l'utilisateur d'une adresse IP spécifique ou, à l'inverse, les adresses IP utilisées par une personne précise. L'identité de l'abonné d'une adresse IP est l'information la plus fréquemment recherchée dans les enquêtes pénales à l'échelle nationale et internationale ayant trait à la cybercriminalité et aux preuves électroniques. Sans ces informations, il est souvent impossible de mener une enquête[31].

[27] Voir les conclusions du rapport suivant : http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf
[28] http://www.coe.int/en/web/deputy-secretary-general/-/increasing-co-operation-against-cyberterrorism-and-other
[29] http://curia.europa.eu/juris/document/document.jsf?text=Data%2BRetention&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=305870#ctx1
[30] Voir à l'annexe pour des informations supplémentaires.
[31] En décembre 2014, le T-CY a adopté une étude sur les « règles concernant l'obtention de données relatives aux abonnés », faisant observer que les données relatives aux abonnés sont la catégorie de données la plus souvent

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, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services[32] 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. »

Au terme de l'évaluation des dispositions concernant l'entraide, le T-CY a recommandé d'envisager un régime plus souple pour les demandes internationales pour une série limitée de données relatives aux abonnés[33] :

> « Recommandation 19 : Les Parties devraient considérer permettre – via des amendements juridiques nationaux et accord international – pour la divulgation rapide de l'identité et l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur. »

Les données relatives aux abonnés comprennent également les données tirées de bureaux d'enregistrement sur les déposants de noms de domaines[34].

Les données relatives aux abonnés sont généralement détenues par le fournisseur de services « offrant des prestations sur le territoire de la Partie », bien que les informations puissent être en fait stockées sur des serveurs situés dans d'autres juridictions[35]. Il arrive parfois que l'on ne sache pas clairement à qui adresser une demande de données relatives aux abonnés. Cela étant, l'article 18.1.b de la Convention de Budapest offre une solution pratique en ce que les autorités compétentes d'une Partie doivent pouvoir demander des données relatives aux abonnés auprès d'un fournisseur de

---

recherchée dans le cadre des enquêtes menées sur le territoire national mais aussi au niveau international. Le T-CY a pris note de diverses règles pour l'obtention de données relatives aux abonnés selon lesquelles, dans certaines Parties, les données relatives aux abonnés sont traitées de la même façon que les données relatives au trafic – en particulier concernant les adresses IP dynamiques – tandis que dans d'autres Parties, les conditions d'obtention de données relatives aux abonnés sont moins strictes. Le T-CY a recommandé « une plus grande harmonisation entre les Parties concernant les conditions, les règles et les procédures pour l'obtention de données relatives aux abonnés ».
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
Voir à la page 123 du rapport suivant :
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[32] Dans le présent document, le terme « fournisseur de services » est utilisé au sens de l'article 1.c de la Convention de Budapest.

[33] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[34] Pour plus d'informations sur le sujet, voir la discussion sur les recommandations relatives à la répression faites à l'ICANN et sur la question de la précision de WHOIS. Voir l'explication du processus d'enregistrement de domaine à l'adresse suivante : http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercriminalité/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter2.pdf

[35] Par exemple, Google compte plusieurs centres de données en Europe (http://www.google.com/about/datacenters/inside/locations/index.html) ; Microsoft en a « plus d'une centaine », 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, et Facebook a également un centre de données en Suède https://www.facebook.com/LuleaDataCenter

service offrant des prestations sur son territoire indépendamment du lieu où les informations sont en fait stockées :

> 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.

En Belgique, cette compétence traduite dans le Code d'instruction criminelle à l'article 46bis, paragraphe 2, est mise en cause dans l'affaire Yahoo! Belgique[36].

2.4.2 Données relatives au trafic

Les fichiers où sont enregistrées les activités du système d'exploitation d'un ordinateur ou d'autres logiciels ou les communications entre des ordinateurs sont essentiels pour l'analyse informatique forensique et les enquêtes sur la cybercriminalité. Cela inclut en particulier les « données relatives au trafic », telles que définies 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 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 de service sous-jacent ».

Les données relatives au trafic peuvent aussi aider à déterminer l'emplacement physique de systèmes informatiques et, par conséquent, d'utilisateurs.

Ces données aussi peuvent être détenues par des fournisseurs de services situés dans un pays alors que les données sont en fait conservées sur des serveurs situés dans d'autres pays.

L'article 5 de la directive 2006/24/EC de l'Union européenne[37] sur la conservation de données renseigne plus en détail sur les données jugées nécessaires et associe les données relatives aux abonnés et les données relatives au trafic (voir à l'annexe).

2.4.3 Données relatives au contenu

Les données relatives au contenu sont souvent nécessaires dans les enquêtes pénales. 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, c'est-à-dire le sens de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic). »

[36] http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation
[37] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.
La directive a été invalidée par la Cour européenne de justice en 2014.

Les données relatives au contenu – e-mail, images, films, musique, documents ou autres fichiers – dans le cloud sont détenues par des fournisseurs de services qui offrent des prestations sur le territoire d'une Partie alors qu'elles peuvent en fait être conservées sur des serveurs situés dans d'autres juridictions.

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 doivent être recueillies, par exemple, en interceptant une communication.

L'interception de communications est possible sur injonction d'un tribunal soit directement par la police ou par une structure spécialisée, soit avec l'assistance d'un fournisseur de service. Cette mesure se limite souvent aux infractions graves.

2.5 Informatique dans le cloud

La définition souvent citée d' « informatique dans le cloud » ou « cloud computing » est la suivante :

> « Le cloud computing est un modèle informatique qui permet un accès facile et à la demande par le réseau à un ensemble partagé de ressources informatiques configurables (réseaux, serveurs, stockage, applications, services, etc.) qui peuvent être rapidement provisionnées et libérées par un minimum d'efforts de gestion ou d'interaction avec le fournisseur du service. Ce modèle en nuage privilégie la disponibilité et se compose de cinq caractéristiques essentielles (accès aux services par l'utilisateur à la demande, accès réseau large bande, réservoir de ressources, redimensionnement rapide (élasticité), service à l'usage) ; de trois modèles de service (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)) ; et de quatre modèles de déploiement (cloud privé, cloud communautaire, cloud public et cloud hybride). Les principales technologies du cloud sont notamment : (1) des infrastructures rapides à grande distance ; (2) des serveurs puissants et peu coûteux ; et (3) une virtualisation extrêmement performante pour le matériel de base »[38].

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

> « Dans le domaine de l'expertise informatique traditionnelle, en raison de la nature centralisée du système de technologie de l'information, les enquêteurs peuvent contrôler totalement les objets à expertiser (routeur, logs de process, disques durs). Or, dans l'écosystème du cloud, en raison de la nature décentralisée des systèmes de technologie de l'information, le contrôle des couches fonctionnelles varie selon les acteurs du cloud, en fonction du modèle de service. En conséquence, les enquêteurs ont une visibilité et un contrôle réduits des objets à expertiser. »[39]

3 Défis pour les systèmes de justice pénale

[38] http://www.nist.gov/itl/cloud/
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[39] « NIST cloud computing forensic science challenges » (projet), juin 2014
http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

3.1 Echelle et ampleur de la cybercriminalité, des dispositifs, des utilisateurs et des victimes

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 électronique est consignée et donne lieu à des enquêtes. Les victimes ne peuvent, dans leur grande majorité, espérer que la 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[40].

3.2 Défis techniques

Aux défis que pose l'informatique dans le cloud pour les instances pénales s'ajoutent une variété d'autres éléments problématiques qui rendent les enquêtes extrêmement complexes, à savoir :

- les réseaux pair à pair/les réseaux virtuels privés ;
- les anonymiseurs (TOR, I2P) ;
- le cryptage ;[41]
- la VoIP ;[42]
- la transition IPv4 vers IPv6 et la traduction d'adresses réseau à grande échelle (CGN).[43]

Il y a lieu de traiter ces éléments problématiques séparément et dans le détail.

3.3 Informatique dans le cloud, territorialité et compétence

L'informatique dans le cloud soulève un certain nombre de questions en matière de justice pénale, en particulier de compétence et de droit applicable, notamment :

- l'indépendance du 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 service peut avoir son siège dans un pays et ressortir juridiquement d'un deuxième pays, alors que les données sont stockées dans un troisième pays. 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 à exclure qu'un fournisseur de services dans le cloud déplace systématiquement les données pour empêcher l'accès de la justice pénale.

[40] Sur l'obligation positive de protéger les personnes, voir l'arrêt de la Cour européenne des droits de l'homme dans l'affaire K.U. c. Finlande http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}

[41] Voir Sarah Lowman (2010) à l'adresse suivante : http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf

[42] Voir Muhammad Tayyab Ashraf, John N. Davies et Vic Grout (2011), à l'adresse suivante : http://www.glyndwr.ac.uk/computing/research/pubs/SEIN_ADG.pdf

[43] Voir les informations complémentaires à l'annexe.

- Même si, en théorie, des données peuvent toujours être situées à un endroit lorsqu'elles sont conservées sur des serveurs dans le nuage[44], il est très difficile de savoir clairement quelles règles s'appliquent pour assurer un accès légal aux autorités judiciaires[45]. Il peut être avancé que la compétence est déterminée par le lieu où se trouve le siège du fournisseur de services ou de son sous-traitant, ou le lieu où se trouvent les données et le serveur, ou la législation de l'État dans lequel le suspect s'est abonné à un service, ou encore le lieu où se trouve le suspect ou sa nationalité.
- Dans de nombreux cas, on ne sait pas clairement si un fournisseur de services dans le nuage est responsable du « traitement » ou du « sous-traitement »[46] 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 lorsque les données sont conservées via des systèmes de co-hébergement transnationaux.

▪ Un fournisseur de services peut relever à la fois de différents niveaux de compétence 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[47] semble déterminée par le lieu où se trouve le responsable du traitement des données et non celui où se trouvent le siège

---

[44] https://www.eff.org/files/2014/12/15/computer_science_experts_microsoft_ireland_amicus_brief.pdf. Toutefois, cet amicus curiae ne semble pas analyser pleinement l'impact sur les règles de compétence lorsque « des copies secondaires de données sont sauvegardées sur des serveurs ou dans des centres de données à distance en cas de problème » (p. 21), comme c'est généralement le cas pour assurer la continuité des activités.

[45] Voir l'affaire pendante Microsoft c. Irlande :
http://www.lexology.com/library/detail.aspx?g=ce97dcac-949b-4004-9ae8-8ea716b1e6a5
http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s%20Memorandum%20of%20Law%20in%20Opposition%20to%20Motion%20to%20Vacate%20%28doc%2097....pdf
http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Government%27s%20Memorandum%20of%20Law%20in%20Opposition%20to%20Motion%20to%20Vacate%20%28doc%2097....pdf
https://s3.amazonaws.com/s3.documentcloud.org/documents/1149373/in-re-matter-of-warrant.pdf
https://www.eff.org/files/2014/12/12/microsoft_opening_brief.pdf
http://digitalconstitution.com/wp-content/uploads/2014/12/Ireland-Amicus-Brief.pdf

[46] Article 2 de la Directive 95/46 de l'Union européenne : « Définitions. Aux fins de la présente directive, on entend par :

[…]

(d) « responsable du traitement » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ;

(e) « sous-traitement » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

[47] Article 4 de la Directive 95/46 de l'Union européenne: « Droit national applicable.

1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque :

(a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ;

(b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public ;

(c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même ».

international, les serveurs, les clients ou autres éléments[48]. Toutefois, certaines sociétés n'ont pas de responsables du traitement dans l'Union européenne, même si elles comptent un certain nombre d'utilisateurs en Europe. Dans ce cas, on ne sait pas clairement quelle est la compétence éventuelle des agences européennes de protection des données pour ces services[49]. Le « droit à l'oubli » invoqué dans l'affaire impliquant Google en Espagne se fonde en revanche sur des critères de compétence différents du lieu où se trouvent le siège international, les serveurs et les responsables du traitement des données[50].

- A des fins fiscales, la compétence semble ne pas 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[51].
- Concernant la protection du consommateur, le lieu où se trouve le consommateur semble déterminant[52].
- Concernant les droits de propriété intellectuelle dans le cadre d'affaires civiles, le lieu où se trouve la société semble déterminer la compétence[53], tandis que pour les droits

[48] Par exemple, Facebook a un bureau de traitement des données en Irlande, considéré comme étant placé sous la juridiction de l'Agence de protection des données de l'Irlande. Or, le siège international de Facebook est sis aux Etats-Unis et la société dispose d'un parc de serveurs en Suède pour ses activités en Europe. Dans le cadre d'affaires pénales, la police ou les procureurs doivent adresser une demande d'entraide judiciaire aux Etats-Unis pour obtenir des données relatives au contenu. Ils ne peuvent déposer de demande auprès du bureau irlandais de Facebook, qui relève de la législation irlandaise, ni du bureau en charge du parc de serveurs suédois de Facebook, qui relève de la législation suédoise.
Toutefois, voir également la situation concernant l'Agence de protection des données des Pays-Bas et Facebook, qui illustre la multiplicité des modèles de compétence appliqués ou invoqués :
https://www.cbpweb.nl/en/news/facebook-provides-information-after-formal-demand-dutch-dpa

[49] A titre d'exemples : VK.com (siège en Russie), Baidu (siège en Chine), Snapchat (siège aux États-Unis) et Hushmail (siège au Canada). Toutes ces sociétés recueillent et traitent des données à caractère personnel. VK et Snapchat proposent des services localisés pour plusieurs marchés européens.

[50] Voir l'arrêt de la Cour européenne de justice dans l'affaire Google Espagne c. Costeja et, en particulier, la question de l'application territoriale dans la directive de l'Union européenne 95/46
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN :
« 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 État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État 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 État membre ».

[51] Voir l'arrêt concernant Google Ireland LTD, Google France et l'administration fiscale :
« Le juge des libertés et de la détention a autorisé des agents de l'administration fiscale à procéder à des visites et saisies, sur le fondement de l'article L. 16 B du livre des procédures fiscales, dans des locaux susceptibles d'être occupés par les sociétés Google France et (ou) Google Ireland Limited, en vue de rechercher la preuve de la fraude de cette dernière. Google souhaite faire annuler la procédure. Google estime que les documents saisis, car saisis à partir de l'interconnexion entre les machines se trouvant dans les locaux en France et à l'étranger, qu'il s'agit d'une saisine extra territoriale et de ce fait non valable. Le Juge estime toutefois que les données saisies sont supposées être situées à l'adresse où est localisé l'ordinateur alors même que les données sont situées sur un serveur étranger. »
http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028209493&fastReqId=2089348476&fastPos=2

[52] En 2006, les associations nordiques de protection du consommateur se sont plaintes auprès d'Apple iTunes, société américaine ayant une filiale au Luxembourg, de la pratique consistant à vendre des services aux consommateurs nordiques sans appliquer la législation locale relative à la protection du consommateur. L'un des points de désaccord concernait l'utilisation de la gestion des droits numériques (DRM). Les associations de protection du consommateur ont fait valoir que cela n'était pas juste pour les consommateurs. D'une manière générale, Apple iTunes a invoqué la législation luxembourgeoise et le Luxembourg comme lieu du dépôt de toute plainte. Les associations nordiques de protection du consommateur ont affirmé que cela allait à l'encontre de la législation locale relative aux ventes à distance, d'autant plus que les services iTunes faisaient l'objet d'une localisation – langue, contenus et monnaie utilisée pour le paiement – pour les divers marchés nordiques. Apple iTunes a fini par modifier sa politique (2009). Au final, la compétence a été déterminée par le lieu où se trouve le consommateur ou l'utilisateur final.
http://www.twobirds.com/en/news/articles/2006/itunes-terms-service-scrutiny-nordic-consumer-ombudsmen

[53] Google a décidé en 2014 de fermer son service Google News en Espagne, à la suite de plaintes émanant d'organismes de presse espagnols. D'après ces plaintes, Google News a porté atteinte à leur droit de propriété intellectuelle et devait les rémunérer pour avoir créé et exploité un service reproduisant leur contenu. Les

de propriété intellectuelle dans le cadre d'affaires pénales, le lieu où se trouve l'auteur de l'infraction peut être déterminant[54].

- Le partage et la mise en commun des ressources sont une caractéristique essentielle de l'informatique dans le cloud. Les services proposés dans le nuage peuvent combiner plusieurs modèles de services (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)). Dans de nombreux cas, lorsqu'un ou plusieurs types de services sont proposés, 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 doit faire l'objet d'une injonction de produire.

- Dans de nombreux cas, on ne sait 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 nuage sont considérés et réglementés comme des « services de communications électronique »[55] 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[56].

---

arguments avancés en faveur de la compétence espagnole étaient assez proches de ceux avancés dans l'affaire concernant le « droit à l'oubli », à savoir, concrètement, que Google exploitait une entreprise en Espagne.
http://www.wsj.com/articles/google-shuts-spanish-news-service-ahead-of-new-law-1418728149

[54] L'affaire de « Pirate Bay » en Suède est un exemple parmi d'autres. Comme dans beaucoup d'autres affaires pénales, le lieu où se trouve l'auteur de l'infraction est le facteur déterminant. Si les arguments utilisés dans l'affaire Google Espagne avaient été invocables au pénal, la société et les gérants de Pirate Bay auraient pu être poursuivis dans une quelconque juridiction où ils exerçaient leurs activités. Comme Google News, une partie du revenu de Pirate Bay provenait de la publicité.
http://www.theguardian.com/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict
http://en.wikipedia.org/wiki/The_Pirate_Bay_trial

[55] Voir l'arrêt de la Cour d'appel d'Anvers, 12e chambre, 2012/CO/1054, 20 novembre 2013 (affaire Yahoo! Belgique) :
« La partie défenderesse continue d'affirmer, en vain, qu'elle ne propose pas de services consistant partiellement ou principalement en la transmission de signaux via des réseaux de communication électronique. Elle offre en Belgique, entre autres choses, un service de messagerie (web) qui permet aux personnes inscrites par voie électronique de communiquer par internet en utilisant une adresse IP à partir d'un fournisseur d'accès internet et assure la transmission de cette communication électronique (voir plus bas). Ce processus diffère de ceux que proposent les fournisseurs d'accès internet (à l'instar de Telenet et Belgacom), qui ne donnent accès à internet que par une adresse IP. L'adresse IP attribuée n'est connue cependant que du fournisseur de services internet (à l'instar de Yahoo!). La défense a fait un choix délibéré à des fins commerciales, comme l'a établi, à juste titre, le premier juge : si la défense ne tient pas à faire l'objet des obligations énoncées à l'article 46bis, paragraphe 2 du Code d'instruction criminelle, la défense est libre d'exclure la plage IP en Belgique (voir le nombre en marge 4.3 de la décision opposée).
Le ministère public démontre, documents 2 et 9 à l'appui – sachant qu'il n' y a pas de raison de douter de la crédibilité ni de l'objectivité de ces documents – que l'envoi d'un e-mail de l'expéditeur au destinataire s'effectue principalement si ce n'est uniquement via les serveurs de messagerie de la partie défenderesse et que lorsque qu'un e-mail est envoyé d'un compte Yahoo! vers un autre compte Yahoo! aucun autre service n'est même utilisé, ce qui prouve que la partie défenderesse est le principal ou l'unique fournisseur de son service de messagerie électronique pour la transmission de signaux via des réseaux de communication électronique. Ces conclusions ne sont pas contestées par Jonas Mariën, expert de la partie défenderesse, ni par les arguments divergents de cette dernière.
Contrairement aux déclarations contenues dans les conclusions de la partie défenderesse (page 6), cette dernière était capable de toute évidence de se défendre contre l'argumentaire de la partie poursuivante (notamment, en consultant son propre expert), ce qui permet d'affirmer que ses droits n'ont pas été enfreints (article 6 de la CEDH).
Le fait que la partie défenderesse offre ses services de messagerie électronique en Belgique est renforcé par le fait qu'elle envoie des messages publicitaires tenant compte du lieu concerné et de la langue. De plus, www.yahoo.be semble offrir les mêmes services que www.yahoo.com par le passé.
Les faits ont donc été prouvés ».

[56] Alors que la Convention de Budapest ne fait pas cette distinction et les considère tous comme des « fournisseurs de services » (article 1.c). La directive 2000/31/CE sur le commerce électronique couvre les « services de la société de l'information » tandis que la directive sur la vie privée et les communications électroniques et la (désormais caduque) directive sur la conservation des données couvrent les « services de

- Pour ce qui est des interceptions, 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.
  - 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 au plan juridique[57].

- 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 nuage (mutualisation, distribution et séparation des données) et des enjeux juridiques liés à l'intégrité et à la validité de la collecte de données, au contrôle des éléments de preuve, à la propriété des données et à la compétence[58].

3.4 Entraide judiciaire

L'entraide judiciaire demeure le principal moyen d'obtenir des éléments de preuve auprès de juridictions étrangères à des fins de procédures pénales. En décembre 2014, le comité de la Convention Cybercriminalité (T-CY) a mené une évaluation du fonctionnement des dispositions concernant l'entraide judiciaire[59]. Il a conclu notamment que :

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

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

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

---

communication électronique ». Par exemple, les services de messagerie électronique ne sont pas considérés nécessairement comme des services de communication électroniques et ne relevaient donc pas de la directive sur la conservation des données.
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=en
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[57] Voir l'article 20 de la Convention européenne d'entraide judiciaire en matière pénale, qui prévoit une notification et validation a posteriori.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF

[58] NIST cloud computing forensic science challenges (projet) juin 2014.
http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

[59] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

4 Questions

Le présent document de réflexion attire l'attention sur les défis complexes auxquels les autorités judiciaires sont confrontées pour obtenir l'accès aux preuves électroniques stockées dans le nuage.

Il convient de clarifier plusieurs points et de s'accorder sur des solutions complémentaires pour s'assurer que les autorités judiciaires sont en mesure de protéger la société et les personnes, ainsi que leurs droits, contre la criminalité.

Il peut être utile d'échanger sur les questions suivantes pour faire avancer la réflexion :

4.1 Compétence

1. Quel gouvernement serait le destinataire d'une demande légale de données adressée par un pays victime d'une cyberattaque dans le nuage dont le pays d'origine n'est pas clair, 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 ?

2. 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 ? Le lieu où se trouve le responsable du traitement des données ? Le lieu où se trouve le siège du fournisseur de services dans le nuage ou sa filiale ? Le pays où un fournisseur de services dans le nuage offre ses prestations ? La législation du pays où le propriétaire des données s'est abonné à un service ? Le pays des autorités judiciaires ?

3. Qu'entend-on par « offrant des prestations sur le territoire de la Partie » (article 18.1.b de la Convention de Budapest)[60] ?

4. Si une injonction de 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 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 ?

4.2 Entraide judiciaire

5. 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 à augmenter considérablement les ressources disponibles pour assurer un traitement efficient des demandes d'entraide judiciaire au niveau des autorités centrales

[60] 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.

compétentes mais aussi des tribunaux locaux et des services de poursuite et de police où les demandes sont préparées et exécutées ?

6. 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 ?

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

8. 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 inconnus dans le cadre d'enquêtes pénales spécifiques[61] ? Par exemple :

   - Rec 19 Les Parties devraient envisager d'autoriser – par des amendements juridiques nationaux et un accord international – la divulgation rapide de l'identité et de l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur.

   - Rec 20 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.

   - Rec 21 Les Parties devraient envisager de renforcer la coopération directe entre autorités judiciaires pour ce qui concerne les demandes d'entraide.

   - Rec 22 Les Parties devraient envisager de traiter la pratique des services répressifs et judiciaires pour l'obtention de données relatives au trafic et aux abonnés directement auprès des fournisseurs de services étrangers, sous réserve de garanties et de conditions.

   - Rec 23 Les Parties devraient étudier la possibilité d'enquêtes conjointes et/ou la création d'équipes d'enquête conjointes.

   - Rec 24 Les Parties devraient envisager de permettre que les demandes soient envoyées en anglais, en particulier les demandes de conservation.

   - Les solutions déjà en place ou les principes déjà reconnus dans d'autres instruments internationaux devraient être pris en compte[62].

Ces questions pourront notamment servir de base aux discussions de la conférence Octopus sur la coopération contre la cybercriminalité, qui se tiendra du 17 au 19 juin 2015 (www.coe.int/octopus2015).

[61] Voir par exemple les recommandations 19 à 24 à la page 127 du document http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[62] Par exemple dans : le Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale (STE 182) du Conseil de l'Europe http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG ;
la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF ;
la décision d'instruction européenne dans les affaires criminelles http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

5 Annexe

5.1 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[63] établi par la décision du T-CY adoptée lors de la 12e Réunion Plénière (2-3 décembre 2014)
Durée	1er 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. Le groupe de travail prépare un rapport pour examen par le T-CY, prenant en compte : ▪ 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) ; ▪ les travaux du sous-groupe ad hoc sur l'accès transfrontalier aux données et sur les questions de compétence territoriale ; ▪ 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. Le rapport doit contenir des propositions d'options et des recommandations d'actions futures du T-CY.
Indicateurs et éléments livrables	▪ Juin 2015 : document de travail contenant une description des défis actuels et émergents qui servira de base à un échange de vues avec les fournisseurs de services et d'autres intervenants à la Conférence Octopus 2015. ▪ Juin 2015 : atelier à la Conférence Octopus. ▪ Décembre 2015 : rapport intérimaire aux fins d'examen par le T-CY. ▪ Juin 2016 : projet de rapport pour examen par le T-CY. ▪ Décembre 2016 : rapport final pour examen par le T-CY.
Méthodes de travail	Le groupe de travail doit se réunir immédiatement après les réunions du Bureau T-CY et à huis clos. Le groupe de travail peut tenir des audiences publiques, publier des résultats provisoires et consulter d'autres parties concernées.
Composition	• Les membres du Bureau participent d'office avec prise en charge des frais[64] • Jusqu'à cinq membres supplémentaires avec prise en charge des frais[65] • Membres additionnels du T-CY (Etats parties) à leurs propres frais.

[63] http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercriminalité/TCY/TCY%202013/T-CY%282013%2925%20rules_v15.pdf
[64] Sous réserve de la disponibilité de financements.
[65] Sous réserve de la disponibilité de financements.

5.2 Notes sur les « données relatives aux abonnés »

Les données relatives aux abonnés sont essentielles pour identifier l'adresse d'utilisateurs d'un protocole internet spécifique (IP) ou, inversement, les adresses IP utilisées par une personne spécifique.

> L'identification de l'abonné auquel se rapporte une adresse IP utilisée est l'information la plus souvent recherchée dans le cadre des enquêtes pénales nationales et internationales en matière de cybercriminalité et de preuve électronique. Elle est, la plupart du temps, déterminante pour établir la vérité : sans cette information préliminaire, il est bien souvent impossible de poursuivre l'enquête.[66]

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, 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.

Le paragraphe 178 du rapport explicatif de la Convention de Budapest précise que, dans le cadre d'une enquête pénale, les données 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.

Le paragraphe 178 poursuit :

> 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.

[66] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
Voir à la page 123 du document publié à l'adresse suivante :
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

Le paragraphe 180 du rapport explicatif clarifie la gamme de données à considérer comme des données relatives aux abonnés :

> 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.

En décembre 2014, le T-CY a adopté une étude sur les « règles concernant l'obtention de données relatives aux abonnés », en attirant l'attention sur le fait que ce type de données est le plus recherché dans les enquêtes menées à l'échelle nationale et internationale[67]. Le T-CY a relevé des règles diverses et variées pour l'obtention de données relatives aux abonnés selon lesquelles dans certaines Parties, ces données sont menacées au même titre que les données relatives au trafic – surtout en lien avec les adresses IP dynamiques –, alors que, dans d'autres, les conditions d'obtention de ces données sont moins strictes.

Le T-CY recommande de fait « une plus grande harmonisation entre les Parties sur les conditions, règles et procédures pour l'obtention de données relatives aux abonnés ».

Au terme de l'évaluation de l'entraide judiciaire, le T-CY a recommandé d'envisager un régime simplifié pour les demandes internationales concernant un nombre limité de données relatives aux abonnés[68] :

> Recommandation 19 : Les Parties devraient envisager d'autoriser – par des amendements juridiques nationaux et un accord international – la divulgation rapide de l'identité et l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur.

Les données relatives aux abonnés sont détenues par des fournisseurs de service qui offrent des prestations sur le territoire de la Partie, bien que les informations puissent être en fait stockées sur des serveurs situés dans d'autres juridictions[69]. Il arrive parfois que l'on ne sache pas clairement à qui adresser une demande de données relatives aux abonnés. Cela étant, l'article 18.1.b de la Convention de Budapest offre une solution pratique en ce que les autorités compétentes d'une Partie doivent pouvoir demander ces données auprès d'un fournisseur de service offrant des prestations sur son territoire indépendamment du lieu où les informations sont en fait stockées :

> 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 :

[67] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2014)17_Report_Sub_Info_v7adopted.pdf
Voir à la page123 du document publié à l'adresse suivante :
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[68] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercriminalité/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[69] Par exemple, Google compte également plusieurs centres de données en Europe (http://www.google.com/about/datacenters/inside/locations/index.html), Microsoft a « plus d'une centaine de centres de données », notamment à Amsterdam et Dublin (http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf), et Facebook, un centre de données en Suède (https://www.facebook.com/LuleaDataCenter).

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.

En Belgique, cette compétence traduite dans le Code d'instruction criminelle à l'article 46bis, paragraphe 2, est mise en cause dans l'affaire Yahoo! Belgique.

5.3 Catégories de données à conserver (Article 5 de la Directive 2006/24/EC de l'Union européenne[70])

Article 5 – Catégories de données à conserver

1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes :

(a) les données nécessaires pour retrouver et identifier la source d'une communication

(1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :

(i) le numéro de téléphone de l'appelant ;

(ii) les nom et adresse de l'abonné ou de l'utilisateur inscrit ;

(2) en ce qui concerne l'accès à internet, le courrier électronique par internet et la téléphonie par internet :

(i) le(s) numéro(s) d'identifiant attribué(s) ;

(ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;

(iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication (a) les données nécessaires pour retrouver et identifier la source d'une communication ;

(b) les données nécessaires pour identifier la destination d'une communication :

(1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile :

(i) le(s) numéro(s) composé(s) [le(s) numéro(s) de téléphone appelé(s)] et, dans les cas faisant intervenir des services complémentaires tels que le renvoi ou le transfert d'appels, le(s) numéro(s) vers le(s)quel(s) l'appel est réacheminé ;

(ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) ;

(2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet :

(i) le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'internet ;

(ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication ;

(c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication :

(1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, la date et l'heure de début et de fin de la communication ;

(2) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :

(i) la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit ;

(ii) la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'internet ou de téléphonie par l'internet dans un fuseau horaire déterminé ;

(d) les données nécessaires pour déterminer le type de communication :

(1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, le service téléphonique utilisé ;

[70] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.
La Directive a été invalidée par la Cour européenne de justice en 2014.

(2) en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet, le service internet utilisé ;

(e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel :

(1) en ce qui concerne la téléphonie fixe en réseau, le numéro de téléphone de l'appelant et le numéro appelé ;

(2) en ce qui concerne la téléphonie mobile :

(i) le numéro de téléphone de l'appelant et le numéro appelé ;

(ii) l'identité internationale d'abonné mobile (IMSI) de l'appelant ;

(iii) l'identité internationale d'équipement mobile (IMEI) de l'appelant ;

(iv) l'IMSI de l'appelé ;

(v) l'IMEI de l'appelé ;

(vi) dans le cas des services anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation (identifiant cellulaire) d'où le service a été activé ;

(3) en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet :

(i) le numéro de téléphone de l'appelant pour l'accès commuté ;

(ii) la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ;

(f) les données nécessaires pour localiser le matériel de communication mobile :

(1) l'identité de localisation (identifiant cellulaire) au début de la communication ;

(2) les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive.

5.4 Transition IPv4 à IPv6 et traduction d'adresses réseau à grande échelle (CGN) [71]

Les fournisseurs de services internet tiennent un registre des adresses IP attribuées aux appareils connectés. En principe, les adresses IP permettent d'identifier un appareil connecté au réseau. Dans le cadre d'enquêtes pénales, il est essentiel de pouvoir remonter jusqu'à un appareil et, de cette façon, jusqu'à un utilisateur.

Compte tenu du nombre limité d'adresses disponibles dans la Version 4 (IPv4) du Protocole internet, il est fréquent, depuis maintenant plusieurs années, que les fournisseurs de services internet n'attribuent pas d'adresse IP stable (statique) à un appareil spécifique d'utilisateur final, mais une série d'adresses IP à un réseau périphérique dans lequel des adresses IP sont alors attribuées de façon dynamique aux appareils qui se connectent au réseau périphérique. Cette attribution dynamique d'adresses IP est possible grâce aux traducteurs d'adresses réseau (« Network Address Translators » ou « NAT »). L'adresse IP mais aussi les « horodatages » sont nécessaires pour déterminer quel appareil utilise une adresse IP à un moment donné et ainsi identifier l'appareil, donc, le client.

La multiplication du nombre d'appareils mobiles pouvant accéder à internet a accéléré l'épuisement des adresses IPv4, problème que la Version 6 du protocole internet (IPv6) est censée résoudre progressivement. La transition d'IPv4 à IPv6 prend plus de temps que prévu et l'on ne sait pas exactement combien de temps elle durera. Pour des raisons de non-rétrocompatibilité, les hébergeurs doivent exploiter les deux protocoles en parallèle lors de cette période de transition. Les fournisseurs de services internet surmontent la pénurie d'adresses IPv4 en généralisant les NAT.

Les traducteurs d'adresses réseau à grande échelle (« Carrier-grade NAT » ou CGN) compliquent la tâche de remonter jusqu'à l'appareil connecté. Les adresses IP et l'horodatage ne suffisent pas, car ils permettent seulement d'identifier le fournisseur de services internet. Des informations complémentaires, y compris en particulier, les adresses de port d'origine et de destination, seraient nécessaires. Les registres produits par les CGN sont très vastes et difficiles à tenir pour les fournisseurs de services internet. Il semblerait que les ports ne soient pas couverts par les dispositions réglementaires en vigueur sur la conservation des données.

La question est d'autant plus complexe que les fournisseurs utilisent des solutions différentes durant la période de transition IPv4 à IPv6 pour exploiter les deux protocoles en parallèle (transition en double pile).

En bref, il est particulièrement complexe d'identifier un appareil et un utilisateur par cet appareil dans un environnement de type CGN.

[71] Voir Geoff Huston (2013) à l'adresse suivante : https://labs.apnic.net/?p=433