www.coe.int/TCY

Strasbourg, le 3 décembre 2014 T-CY (2014)16
(provisoire)

Comité de la Convention Cybercriminalité (T-CY)

Accès transfrontalier aux données et compétence :

options concernant l'action future du T-CY

Rapport élaboré par le
Groupe ad hoc du T-CY sur l'accès transfrontalier aux données
et sur les questions de compétence territoriale
adopté lors de la 12e plénière du T-CY (2-3 décembre 2014)

Sommaire

Contact

Alexander Seger
Secrétaire 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 Courriel : alexander.seger@coe.int

1 Introduction

Le présent rapport a été préparé par le Groupe sur l'accès transfrontalier[1] du Comité de la Convention Cybercriminalité (T-CY) à la suite d'une décision prise par la 10e séance plénière du T-CY (2-3 décembre 2013).

Le « Groupe ad hoc du T-CY sur l'accès transfrontalier aux données et sur les questions de compétence territoriale » (ci-après « Groupe sur l'accès transfrontalier ») a été créé par le T-CY lors de la 6e séance plénière (23-24 novembre 2011).

Il a présenté un long rapport, intitulé *Compétence et accès transfrontalier : quelles solutions ?*[2], à la 8e séance plénière du T-CY, qui a adopté le rapport le 6 décembre 2012.

Ce rapport souligne la nécessité de l'accès transfrontalier, mais aborde aussi les préoccupations et les risques (préoccupations juridiques et politiques, risques concernant les garanties procédurales, conséquences pour les tiers, risques pour la protection des données à caractère personnel, risques pour les opérations de police) auxquels il faudrait répondre si les possibilités d'accès transfrontalier devaient se développer. Il énumère également une série de pratiques qui sont d'ores et déjà mises en œuvre et dont certaines vont au-delà des possibilités limitées prévues par la Convention sur la cybercriminalité.

Le rapport propose trois solutions :

1. une application plus efficace de la Convention de Budapest, en particulier de ses dispositions sur la coopération internationale ;
2. une note d'orientation du T-CY sur l'article 32 ;
3. un protocole additionnel à la Convention de Budapest sur l'accès aux preuves électroniques.

Lors de sa 8e séance plénière, le T-CY a prolongé le mandat du Groupe sur l'accès transfrontalier jusqu'au 31 décembre 2013, ce qui a permis :

- une audition publique à Strasbourg le 3 juin 2013 ;
- un projet de note d'orientation sur l'article 32 ;
- une décision, lors de la 9e séance plénière du T-CY (juin 2013), de commencer les travaux sur un protocole en 2014.

En décembre 2013, le Groupe sur l'accès transfrontalier a présenté son rapport à la 10e séance plénière du T-CY et considéré que :

- une réflexion et un dialogue plus approfondis seront nécessaires avec les autorités chargées de la protection des données, la société civile et les organisations du secteur privé pour concilier l'accès transfrontalier aux données avec les garanties et conditions permettant de protéger les droits des individus et de prévenir les abus ;
- alors que la Convention de Budapest est un traité relatif au domaine pénal, qui couvre des enquêtes pénales spécifiques pertinent de l'article 14, le contexte marqué par les

[1] « Groupe ad hoc sur l'accès transfrontalier aux données et sur les questions de compétence territoriale ».
[2] Pour le rapport complet, voir :
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY%282012%293F_transborder_repV31public_7Dec12.pdf

informations faisant état d'une surveillance de masse pratiquée par les agences nationales de sécurité pourrait nuire à la négociation d'un protocole ;

- Il est possible que l'évaluation par le T-CY des dispositions relatives à la coopération internationale débouche sur des propositions supplémentaires à intégrer dans un protocole à la Convention de Budapest.

Lors de sa 10e séance plénière, le T-CY a suivi ce raisonnement et décidé ce qui suit :

> Point 6 de l'ordre du jour : l'accès transfrontalier aux données
>
> Adopter le rapport présenté par le Groupe sur l'accès transfrontalier pour 2013[3], et donc demander au Groupe sur l'accès transfrontalier :
> - de poursuivre le dialogue avec les intéressés ;
> - de tenir compte des résultats du cycle actuel d'évaluations du T-CY ;
> - sur cette base, de soumettre pour examen à la 12e réunion plénière un rapport contenant des propositions ;
>
> En attendant l'examen de ce rapport, mettre en suspens la décision adoptée à l'occasion de la 9e réunion plénière en ce qui concerne l'élaboration d'un protocole à la Convention.

Le présent rapport résume les résultats des travaux menés par le Groupe sur l'accès transfrontalier[4] en 2014 et présente des propositions à examiner lors de la 12e séance plénière du T-CY (décembre 2014)[5].

2 Activités en 2014

2.1 Liste d'activités du Groupe sur l'accès transfrontalier

En 2014, le Groupe sur l'accès transfrontalier a mené les activités ci-après :

5-6 février 2014, Strasbourg	Réunion du Groupe sur l'accès transfrontalier
28 mai 2014, Strasbourg	Réunion avec le groupe de travail « article 29 » de l'UE sur la protection des données, le contrôleur européen de la protection des données et le Comité consultatif de la Convention 108 (T-PD)
17-18 juin 2014, Strasbourg	Réunion préparatoire à la séance plénière du T-CY
19-20 juin 2014, Strasbourg	Conférence sur la protection des données
24 septembre 2014, Bruxelles	Audition de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (commission LIBE)
8-9 octobre 2014, Strasbourg	Réunion du Groupe sur l'accès transfrontalier

[3] Document (T-CY(2013)30) : http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2930F_Final_transb_rep_V5.pdf

[4] Composition du Groupe sur l'accès transfrontalier en 2014 : Ioana Albani (Roumanie), Andrea Candrian (Suisse), Markko Kunnapu (Estonie), Tsuyoshi Kitagawa (Japon), Erik Planken (Pays-Bas), Justin Millar (Royaume-Uni), Cristina Schulman (Roumanie), Betty Shave (Etats-Unis), Branko Stamenkovic (Serbie) et Pedro Verdelho (Portugal).

[5] Note: le rapport et ses propositions ont été adoptés lors de sa 12ème Réunion Plénière du T-CY (2-3 décembre 2014).

2.2 Réunion avec des représentants des organismes de protection des données

En décembre 2013, le T-CY a reçu une lettre du Groupe de travail « article 29 »[6] de l'UE sur la protection des données, qui contenait une série d'observations expliquant que les propositions examinées par le Groupe sur l'accès transfrontalier n'étaient pas compatibles avec les règles de l'UE en matière de protection des données.

En conséquence, le Groupe sur l'accès transfrontalier a eu une réunion, le 28 mai 2014, avec des représentants du groupe de travail « article 29 », le contrôleur européen de la protection des données et le Comité consultatif de la Convention 108 (T-PD) pour débattre des préoccupations détaillées exprimées dans la lettre.

Les discussions ont confirmé la complexité de la question de l'accès transfrontalier aux données et le fait que les observations faites par le groupe de travail « article 29 » dans sa lettre pouvaient être valables dans certains cas, mais pas dans d'autres.

Les discussions ont porté notamment sur les questions suivantes.

2.2.1 Justice pénale contre sécurité nationale

Les Parties à la Convention de Budapest considèrent qu'il s'agit d'un traité de droit pénal qui doit être utilisé pour des enquêtes pénales spécifiques et pour des données spécifiques, et non à des fins de sécurité nationale ou de surveillance massive.

Le groupe de travail « article 29 » questionne cette vision et met en avant le rôle joué par les autorités pénales dans les mesures de sécurité nationale et le partage de données entre les autorités pénales et les autorités chargées de la sécurité nationale.

Il devrait être clair que la Convention de Budapest ne permet pas en bloc un accès transfrontalier, la collecte de données ou le transfert de données. Cependant, si les possibilités d'accès transfrontalier pour des enquêtes pénales spécifiques se développaient, il faudrait prévoir des garanties supplémentaires.

2.2.2 Cadre applicable en matière de protection des données

Le groupe de travail « article 29 » estime que la directive 95/46/CE[7] s'applique aux transferts réalisés par des organismes du secteur privé vers les autorités répressives, tandis que la décision-cadre 2008/977/JAI[8] s'applique aux transferts internationaux de données entre autorités répressives.

---

[6] L'article 29 de la Directive 95/46/CE du 24 octobre 1995 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 (JO L 281, 23.11.1995, p. 31) crée un groupe de protection des personnes à l'égard du traitement des données à caractère personnel. Ce groupe de travail « article 29 » a un caractère consultatif et indépendant. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

[7] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML

[8] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:fr:PDF

Néanmoins, il se pose toute une série de questions quant aux règles de protection des données applicables dans un contexte pénal[9].

On peut se demander pourquoi la directive 95/46/CE serait applicable si la question de l'accès transfrontalier était régie par un traité de droit pénal dont les dispositions seraient transposées dans le droit pénal national. La question a été posée de savoir pourquoi cela ne constituerait pas une dérogation légitime conforme à l'article 13 de la directive 95/46/CE ou à l'article 9 de la Convention 108 sur la protection des données.

D'autres questions ont été soulevées, notamment s'il y a une différence selon que des données sont transférées par des organismes du secteur privé vers des services répressifs au sein des Etats membres de l'UE, ou depuis des Etats membres de l'UE vers des Etats ne faisant pas partie de l'UE, ou depuis des Etats ne faisant pas partie de l'UE vers des Etats membres de l'UE.

Les discussions sur ce point n'ont pas été concluantes. Compte tenu de la réforme en cours du cadre de protection des données dans l'UE et au Conseil de l'Europe[10], certaines de ces questions risquent de rester ouvertes pour le moment.

2.2.3 Droit et garanties applicables

L'un des points les plus difficiles concernant l'accès transfrontalier aux données semble être la question du droit applicable.

Dans sa lettre de décembre 2013, le groupe de travail « article 29 » estime que le droit applicable est celui de l'Etat faisant l'objet de la perquisition (c'est-à-dire l'Etat dans lequel se fait l'accès aux données) :

- « L'application du droit national de la Partie requise signifie que les critères à respecter dans le cadre des enquêtes nationales devront également être respectés dans le cadre des enquêtes transnationales. Il s'agit donc d'une garantie pour les droits des individus. »
- « Le droit de l'UE en matière de protection des données assure la continuité de la protection lorsque des données relevant de l'UE sont transférées à l'étranger. Ces garanties concernant des données traitées dans l'UE ne peuvent être contournées en appliquant le droit de pays tiers à des données traitées dans l'UE. »
- « Un protocole additionnel à une convention internationale qui prévoirait l'accès à des données stockées dans des ordinateurs à l'étranger en appliquant le droit (ou les définitions du consentement) de la Partie effectuant la perquisition serait contraire à l'acquis de l'UE en matière de protection des données. »

Les discussions :

- ont donné à penser que l'approche selon laquelle le droit applicable est celui de l'Etat faisant l'objet de la perquisition pouvait être valable dans certains cas, mais sans garantir une meilleure protection des droits de l'individu dans d'autres situations ;

[9] Il convient de noter le préambule de la décision-cadre 2008/977/JAI :
« La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 (3) ne s'applique pas au traitement des données à caractère personnel dans le cadre d'une activité qui n'entre pas dans le champ d'application du droit communautaire, comme les activités prévues par le titre VI du traité sur l'Union européenne, **et en tout cas pas aux opérations de traitement concernant la sécurité publique, la défense, la sécurité de l'État ou les activités de l'État en matière pénale**. »

[10] http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp

- n'ont pas été concluantes sur la notion de « consentement », qui peut être appliquée différemment en vertu des règles de protection des données par rapport à un contexte pénal.

2.2.4 Capacité des prestataires de services à divulguer des données

Le groupe de travail « article 29 » estime qu'un organisme du secteur privé remplissant la fonction de responsable du traitement des données ne pourrait divulguer des données à caractère personnel volontairement, mais uniquement sur présentation d'une ordonnance judiciaire.

Le Groupe sur l'accès transfrontalier est d'accord sur le principe avec cette position. Néanmoins, il peut y avoir des cas dans lesquels un fournisseur de services internet ou un autre responsable du traitement des données pourrait divulguer des données (dans des situations d'urgence, si le responsable du traitement des données a connaissance d'une infraction, si le fournisseur de services internet est attaqué, si les règles commerciales l'exigent, etc.). L'affirmation selon laquelle un responsable du traitement des données ne peut « jamais » divulguer volontairement des données est inexacte.

L'article 3.6 du projet de note d'orientation (voir annexe) reflète cette idée :

> 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. En général, les prestataires de services ne sont que les dépositaires de ces données. Ils n'en ont pas le contrôle ni la propriété et ne sont donc pas dans la capacité de donner un consentement valide. En revanche, les forces de l'ordre pourront bien sûr se procurer les données dans un pays étranger par d'autres moyens, comme l'entraide judiciaire ou les procédures applicables aux situations d'urgence.

2.2.5 Régulation ou laisser-faire

Il semble qu'un nombre croissant de pays – notamment au sein de l'UE – adoptent des mesures unilatérales pour obtenir l'accès à des données conservées dans des lieux étrangers ou inconnus à des fins pénales pour protéger des personnes contre la criminalité, notamment contre des atteintes à la vie privée (attaques contre la confidentialité, l'intégrité et la disponibilité des ordinateurs (articles 2–6 de la Convention de Budapest), infractions de type cyberharcèlement ou sextorsion).

Les discussions ont fait apparaître une position commune selon laquelle le fait de laisser les Etats adopter leurs propres solutions, unilatérales, risque de créer une situation confuse, tandis que ne rien faire entraînerait une augmentation de la criminalité et des violations des droits fondamentaux.

Il serait par conséquent préférable d'élaborer des solutions internationales qui permettent des mesures pénales efficaces assorties des garanties et conditions nécessaires.

2.3 Conférence sur les garanties de l'article 15 et l'accès des services de répression aux données (19-20 juin 2014)[11]

En décembre 2013, le T-CY a décidé de poursuivre le dialogue avec les parties prenantes intéressées. Une conférence – organisée dans le cadre du projet Cybercrime@Octopus – faisant suite à cette décision s'est tenue à Strasbourg les 19 et 20 juin 2014.

La conférence a porté sur les questions suivantes :

> Pour des enquêtes spécifiques, les autorités judiciaires ont constamment, et de plus en plus, besoin de preuves électroniques provenant d'autres pays. Comment obtenir ces preuves rapidement en respectant les exigences de l'Etat de droit et les normes relatives à la protection des données ? Comment obtenir ces preuves lorsque les procédures d'entraide judiciaire ne sont pas efficaces ? L'amélioration de l'efficacité de la coopération internationale et l'adaptation des règles et procédures pour obtenir rapidement des preuves électroniques éphémères sont considérées comme des questions urgentes.

Pour faciliter l'échange de vues, la conférence était axée sur les points suivants :

- la distinction entre les enquêtes spécifiques visant à obtenir des données à des fins pénales précises et la surveillance et les autres activités menées par les agences nationales de sécurité ;
- le défi de l'accès des services répressifs aux données, compte tenu des évolutions technologiques et des tendances en matière de criminalité ;
- la protection des données et les autres garanties relatives aux droits de l'homme et à l'Etat de droit ;
- les solutions possibles pour concilier l'obligation des Etats de protéger les individus et la société contre la criminalité avec le respect des garanties.

L'audition a montré toute la complexité de la question. Si certains participants ont rejeté d'emblée toute possibilité d'accès transfrontalier aux données, d'autres ont souligné qu'il fallait trouver des solutions communes tenant compte des avancées technologiques, de l'évolution de la cybercriminalité et de la nécessité d'adopter des règles internationales plus claires pour encadrer des pratiques déjà très répandues.

L'audition devait contribuer à trouver des solutions à l'accès transfrontalier aux données tout en répondant aux préoccupations telles que les droits procéduraux des individus et la protection des données à caractère personnel. Elle a permis de tirer des enseignements utiles, notamment au sujet des limites fixées au sujet du consentement volontaire des prestataires de services à divulguer des données.

Fait important, le Groupe sur l'accès transfrontalier a élaboré différents cas de figure[12] pour obtenir des éclaircissements sur les règles applicables en matière de protection des données dans des situations spécifiques. Ces scénarios ont facilité la tenue d'un échange de vues ouvert, même si les réponses aux questions ont généralement été peu concluantes.

---

[11] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/3021_Art15Conf_Agenda_v8.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_art15Conf_Conclusions_v1e.pdf

[12] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/cyber_COE_TB_Scenarios_june2014%20V5web.pdf

Le président de la réunion a résumé les conclusions de la conférence comme suit :

- Les travaux du T-CY sur l'accès transfrontalier aux données s'inscrivent dans une série d'activités menées par le T-CY pour soutenir la mise en œuvre de la Convention de Budapest afin de protéger la société et les personnes contre la criminalité, de préserver leurs droits et de promouvoir l'Etat de droit dans le cyberespace.
- Il est entendu que la Convention de Budapest est un traité de droit pénal qui s'applique à des enquêtes pénales spécifiques et à des données spécifiques.
- L'accès aux preuves électroniques qui se trouvent dans des juridictions étrangères est régi principalement par des accords d'entraide judiciaire. L'évaluation du fonctionnement des dispositions d'entraide judiciaire qui est réalisée actuellement par le T-CY pour en améliorer l'application est un point positif.
- Du fait des évolutions technologiques et de la volatilité des preuves électroniques, les procédures d'entraide judiciaire ne sont pas toujours efficaces ou utiles. Les données peuvent être conservées dans des lieux inconnus, être fragmentées ou être transférées entre de multiples endroits ou juridictions, ce qui limite la capacité des autorités judiciaires à protéger la société et les personnes contre la criminalité.
- Grâce à son article 32, la Convention de Budapest permet un accès transfrontalier aux données dans certaines situations.
- Les Etats élaborent de plus en plus des solutions unilatérales pour accéder à des données dans des juridictions étrangères ou inconnues ne relevant pas des dispositions de la Convention de Budapest. Des solutions doivent être trouvées pour poser une base juridique internationale.
- Ces solutions doivent prévoir des garanties, des conditions et le respect de l'Etat de droit et des principes des droits de l'homme, notamment la protection des données.
- Les conditions en question sont notamment que les prérogatives permettant d'accéder aux données ou autorisant les flux transfrontières de données soient prévues par la loi, visent un objectif légitime et soient proportionnées dans une société démocratique. Cela aidera à éviter des conflits entre la protection des données et le droit pénal.
- Les principes et dispositions de la Convention 108 sur la protection des données et de la Recommandation R(87)15 peuvent aider le T-CY pour la suite de ses travaux. Il est avancé que l'adhésion à la Convention 108 sur la protection des données par les Parties à la Convention de Budapest serait une bonne chose.
- Des solutions sont effectivement nécessaires pour permettre aux autorités judiciaires d'obtenir des preuves électroniques de manière efficace et dans le respect des normes relatives à la protection des données et à l'Etat de droit. Le dialogue constructif visant à élaborer ces solutions devrait par conséquent se poursuivre.

2.4 Audition de la commission LIBE (24 septembre 2014)

Le 12 février 2014, la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a adopté un « rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures »[13] préparé par le rapporteur Claude Moraes.

Si le rapport porte essentiellement sur la surveillance de masse, il est également très critique à l'égard des travaux menés par le T-CY sur l'accès transfrontalier aux données :

[13] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=FR

Le Parlement européen….

32. souligne ses vives inquiétudes face aux travaux en cours au sein du comité de la convention cybercriminalité du Conseil de l'Europe sur l'interprétation de l'article 32 de la convention cybercriminalité du 23 novembre 2001 (convention de Budapest) concernant l'accès transfrontalier à des données informatiques stockées avec autorisation ou lorsque le public peut les consulter, et s'oppose à la conclusion de tout protocole additionnel et à la formulation de toute orientation visant à élargir le champ d'application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception de taille au principe de territorialité, en ce qu'il pourrait donner aux autorités répressives la possibilité d'accéder librement à distance aux serveurs et aux systèmes informatiques situés dans d'autres juridictions sans avoir recours aux accords multilatéraux et aux autres instruments de coopération judiciaire mis en place pour garantir les droits fondamentaux des personnes physiques, y compris la protection des données et l'application régulière de la loi, et notamment la convention n° 108 du Conseil de l'Europe ;

Le rapport est basé sur de nombreuses auditions et contributions d'experts, comme l'indique l'Annexe II du rapport. Or, l'avis du T-CY n'a pas été sollicité avant la finalisation et l'adoption du rapport.

En août 2014, le Secrétariat de la commission LIBE a invité le Secrétariat du T-CY à une « mini-audition » à Bruxelles le 24 septembre 2014. Le président du T-CY, Erik Planken, et le secrétaire exécutif, Alexander Seger, se sont exprimés devant la commission LIBE. Les autres orateurs incluaient notamment Giovanni Buttarelli, assistant du contrôleur européen de la protection des données, et Wojciech Wiewiórowski, inspecteur général de la protection des données personnelles, autorité polonaise de protection des données, vice-président du groupe de travail « article 29 »[14].

L'audition a été assez controversée.

Tandis que la délégation du T-CY a souligné entre autres que la Convention de Budapest est un traité de droit pénal utilisé dans le cadre d'enquêtes pénales, que l'objectif d'un protocole serait également de prévenir une situation confuse et des affirmations de compétence intempestives en créant un cadre légitime comportant des garanties et des conditions, que le dialogue avec les autorités chargées de la protection des données et d'autres parties prenantes vise à définir ces garanties et conditions, qu'il faut trouver des solutions constructives pour protéger les personnes contre la criminalité également dans les situations où l'entraide judiciaire n'est pas applicable, et qu'il n'est pas question d'autoriser un « accès libre » aux données, les membres de la commission LIBE ont maintenu leur position déjà exprimée au paragraphe 32 de leur rapport de février 2014.

En conclusion, il semblerait que :

- la commission LIBE ait utilisé cette occasion pour réaffirmer sa position ;
- il règne une confusion entre la sphère de la justice pénale et celle de la sécurité nationale. La méfiance générale à l'égard des gouvernements compliquera la négociation de nouveaux accords internationaux pour résoudre les problèmes auxquels sont confrontées les autorités judiciaires ;
- il est peu probable que le Parlement européen soutienne la négociation de nouveaux accords avant l'adoption du paquet de mesures sur la protection des données. Il serait

[14] En octobre 2014, Mr. Buttarelli a été nommé Contrôleur européen de la Protection des données ("CEPD"), and Mr. Wiewiórowski Assistant CEPD.

par conséquent compliqué pour la commission européenne d'obtenir un mandat de négociation d'un protocole sur l'accès transfrontalier aux données.

2.5 Evaluation par le T-CY des dispositions sur la coopération internationale

Dans son rapport de décembre 2012, le Groupe sur l'accès transfrontalier avait indiqué qu'une solution résiderait dans « une application plus efficace de la Convention de Budapest, en particulier de ses dispositions sur la coopération internationale ».

Le T-CY a ainsi chargé le Groupe sur l'accès transfrontalier de tenir compte des résultats de ses évaluations des dispositions sur la coopération internationale réalisées en 2013/2014.

Le projet de rapport sur l'évaluation par le T-CY de l'article 31 et des dispositions connexes contient un certain nombre de dispositions spécifiques. Certaines sont d'ordre pratique et pourraient être mises en œuvre rapidement, d'autres nécessitent des moyens supplémentaires au niveau national, et d'autres encore peuvent éclairer un protocole additionnel à la Convention de Budapest.

Certaines questions examinées par le Groupe sur l'accès transfrontalier entre 2012 et 2014 pourraient être traitées dans le cadre des suites données à ces recommandations.

2.6 Note d'orientation sur l'article 32

En février 2013, le Groupe sur l'accès transfrontalier a rédigé un projet de note d'orientation pour examen lors de l'audition publique et lors de la 9e séance plénière du T-CY en juin 2013.

A partir des commentaires recueillis pendant ces réunions et à la suite de nouvelles discussions en son sein, le Groupe sur l'accès transfrontalier a préparé un nouveau projet de note d'orientation (version du 9 octobre 2014)[15]. Cette nouvelle mouture :

- souligne que l'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques, au sens de l'article 14 de la Convention de Budapest ;
- note au point 3.6 que les prestataires de services ne pourront en principe donner leur consentement valable et volontaire à la divulgation des données des utilisateurs en vertu de l'article 32b ;
- indique au point 3.5 que les services répressifs ne doivent pas invoquer l'article 32b pour prendre des mesures contraires au droit interne ;
- note au point 3.7 que l'article 32b ne s'applique pas aux injonctions de produire au niveau national ;
- propose au point 3.3 que les Parties envisagent d'informer les autorités compétentes de la Partie qui fait l'objet de la perquisition, ce qui constituerait une garantie supplémentaire pour protéger les droits des individus et les intérêts des tiers.

Il est proposé que le T-CY examine en séance plénière cette version du projet de note d'orientation en vue de son adoption.

[15] Le projet de note d'orientation est joint en annexe. Il est aussi disponible à l'adresse suivante : http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297F_REV_GN3_transborder_V13.pdf

3 Conclusions et options

3.1 Note d'orientation sur l'article 32

Il est proposé que le T-CY examine en séance plénière le projet de note d'orientation en vue de son adoption.

3.2 Protocole additionnel à la Convention sur la cybercriminalité relatif à l'accès transfrontalier aux données

Le Groupe sur l'accès transfrontalier estime qu'un protocole additionnel sur l'accès transfrontalier aux données serait nécessaire, mais qu'un tel instrument est controversé dans le contexte actuel.

D'après les activités et analyses menées par le groupe, il n'y a pas de consensus raisonnable pour commencer les travaux sur un protocole.

D'un côté,

- les agents de la justice pénale sont extrêmement préoccupés et pleins de ressentiment par rapport à la difficulté d'obtenir des données à des fins de justice pénale et à leur capacité limitée à protéger les individus et la société contre la criminalité ;

- l'augmentation du nombre de personnes et d'activités en ligne s'accompagne d'une augmentation du nombre d'infractions en ligne et de preuves dématérialisées. Pour beaucoup d'infractions, les preuves en ligne sont les seules qui existent ;

- les preuves électroniques occupent une place de plus en plus importante dans le domaine des infractions violentes – meurtres ou viols commandités en ligne, fusillades, attentats, sextorsion, harcèlement ou maltraitance des enfants, entre autres – mais peuvent être stockées dans des juridictions étrangères ou inconnues ;

- de nombreux interlocuteurs ont tendance à négliger les coûts de ce type de criminalité pour les droits de l'homme, notamment en ce qui concerne la vie privée, les conséquences de l'infraction sur la victime et l'obligation positive de l'Etat de protéger les personnes contre la criminalité, y compris la cybercriminalité. Le manque de considération pour les droits des victimes a été une révélation pénible pour le Groupe sur l'accès transfrontalier ;

- les évolutions technologiques, notamment l'informatique en nuage, l'utilisation de nombreux outils et plateformes ou encore le cryptage rendent très complexe la collecte de preuves électroniques à des fins de justice pénale ;

- les procédures d'entraide judiciaire sont inefficaces et rarement applicables ;

- la coopération des prestataires diminue. On constate une tendance chez les prestataires à ne pas coopérer avec des agents de la justice pénale même lorsque la loi le permet, à informer les titulaires des comptes des enquêtes menées par les Etats, à ne pas doter du personnel suffisant leurs services juridiques et à retarder l'exécution des ordonnances judiciaires émises en bonne et due forme ;

- un pourcentage énorme de pistes et d'affaires sont abandonnées, faute de possibilité réaliste d'obtenir ne serait-ce que des données de base comme l'identité du titulaire d'une adresse IP.

Pour toutes ces raisons, la plupart des agents qui s'occupent des questions de justice pénale sont favorables au développement des possibilités d'accès transfrontalier aux données à des fins de justice pénale, avec les garanties nécessaires.

D'un autre côté,

- dans de nombreux gouvernements, certains ministères peuvent être opposés à l'accès transfrontalier aux données si les données se trouvent sur leur territoire, tout en étant indifférents ou en acceptant que leurs propres services aient accès à des données dans d'autres juridictions ;

- les informations faisant état d'une surveillance de masse et d'autres activités menées par les agences nationales de sécurité ont entraîné une perte de confiance dans les gouvernements et une confusion entre les prérogatives et activités de ces agences et celles des autorités judiciaires. Par conséquent, il y aura une réticence publique face aux propositions d'accroître les pouvoirs de la justice pénale. De nombreux gouvernements et parlements seront peu enclins à prendre ce risque en négociant un protocole et en transposant ses dispositions dans le droit national ;

- de nouveaux cadres de protection des données sont toujours en cours d'élaboration dans l'UE et le Conseil de l'Europe. L'espoir que l'UE termine ses travaux avant la mi-2014 ne s'est pas concrétisé. Des travaux supplémentaires sur les régimes de protection des données sont actuellement menés, par exemple entre l'UE et les Etats-Unis (« accord-cadre »[16]) ;

- en Europe, la réglementation relative à l'accès de la justice pénale aux données est floue depuis l'arrêt rendu en avril 2014 par la Cour européenne de justice au sujet de la directive de l'UE sur la conservation de données ;

- la question de l'accès transfrontalier aux données est liée à celle de la compétence. Un certain nombre de faits récents montrent que cette question évolue rapidement et pourrait mériter une analyse plus approfondie[17]. Lors de sa 11e réunion plénière, le T-CY a souligné « l'importance de la question de la compétence et considér[é] de ce fait que les dispositions énoncées à l'article 22 pourraient être évaluées dans le cycle d'évaluations suivant ».

Pour ces raisons et dans le contexte actuel, la négociation d'un protocole sur l'accès transfrontalier aux données ne serait pas faisable.

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

[17] Exemples :
- l'affaire en cours YAHOO!/Belgique ;
- la loi « Marco Civil » adoptée par le Congrès brésilien le 22 avril 2014 soumet les données brésiliennes à la compétence brésilienne, quel que soit le lieu où elles sont stockées. Voir article 11 : http://www.internetjurisdiction.net/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014-PROVIDED-BY-CGIbr.pdf ;
- aux Etats-Unis, en avril 2014, un tribunal de district a élargi le champ d'application du mandat de perquisition, estimant qu'il s'applique « n'importe où » (http://www.theregister.co.uk/2014/04/28/us_judge_digital_search_warrants_apply_everywhere/), compte tenu du fait que l'impossibilité d'obtenir l'accès à des données stockées sur des serveurs à l'étranger en raison de l'inefficacité de procédures d'entraide judiciaire alourdirait « sensiblement la charge pesant sur le gouvernement et entraverait nettement les efforts des services répressifs ».

En même temps, les problèmes ci-dessus ne vont pas disparaître mais plutôt s'amplifier.

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.

De plus, avec le développement de la victimisation, le public demandera pourquoi les gouvernements sont incapables d'obtenir des données d'une manière raisonnable et légitime lorsque des vies sont en danger et pourquoi, souvent, la justice ne peut être rendue.

Le T-CY devrait par conséquent être attentif à la suite des événements et réexaminer à l'avenir la faisabilité d'un protocole consacré à la question spécifique de l'accès transfrontalier aux données.

3.3 Option à soumettre au T-CY

Entre-temps, le T-CY pourrait travailler sur l'option suivante :

A titre de suivi des travaux du Groupe sur l'accès transfrontalier et des évaluations des dispositions sur la coopération internationale, le T-CY pourrait envisager de créer un groupe de travail sur l'accès de la justice pénale aux preuves stockées dans le nuage, notamment dans le cadre d'une entraide judiciaire (« groupe sur les preuves dans le nuage »).

Ce groupe serait principalement chargé d'explorer des solutions concernant l'accès de la justice pénale à des preuves stockées sur des serveurs dans le nuage et dans des juridictions étrangères, notamment dans le cadre d'une entraide judiciaire.

Le groupe de travail rédigerait un rapport à soumettre au T-CY, en s'appuyant sur :

- les recommandations figurant dans le rapport d'évaluation du T-CY concernant les dispositions de la Convention de Budapest sur l'entraide judiciaire (document T-CY(2013)17rev) ;
- les travaux du Groupe ad hoc sur l'accès transfrontalier aux données et sur les questions de compétence territoriale ;
- 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 rapport devrait proposer des options et des recommandations au T-CY.

Le groupe de travail pourrait être créé pour une période de deux ans (voir projet de mandat en annexe).

4 Annexe

4.1 Projet de note d'orientation sur l'article 32[18]

www.coe.int/TCY

Strasbourg, version 9 octobre 2014 T-CY (2013)7 F rev

Comité de la Convention Cybercriminalité(T-CY)

Note d'orientation du n° 3
Accès transfrontalier aux données (article 32)

Proposition établie par le Groupe transfrontalier pour examen par le T-CY

[18] http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297F_REV_GN3_transborder_V13.pdf

1 Introduction

Lors de sa 8e session plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions juridiques, politiques et technologiques.[19]

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes les Parties.

La présente note est consacrée à la question de l'accès transfrontalier aux données tel que visé à l'article 32 de la Convention de Budapest.[20]

L'article 32b énonce une exception au principe de territorialité en autorisant dans des circonstances limitées l'accès transfrontalier unilatéral sans passer par l'entraide judicaire. Les Parties sont invitées à utiliser plus efficacement toutes les dispositions de la Convention de Budapest portant sur la coopération internationale, notamment l'entraide judiciaire.

Dans l'ensemble, les pratiques, les procédures ainsi que les conditions et les garanties qui les accompagnent varient considérablement entre les différentes Parties. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données à caractère personnel, la base légale de l'accès aux données stockées à l'étranger ou au moyen de l'informatique en nuage, et le principe de la souveraineté nationale.

Cette note d'orientation vise à aider les Parties à appliquer la Convention de Budapest, à corriger les malentendus concernant l'accès transfrontalier en vertu de cette convention et à rassurer les tiers.

Elle aidera ainsi les Parties à exploiter pleinement les possibilités offertes par la convention en matière d'accès transfrontalier aux données.

1. Article 32 de la Convention de Budapest

Texte de l'article :

> Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public
>
> Une Partie peut, sans l'autorisation d'une autre Partie :
>
> a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
>
> b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement

[19] Voir le mandat du T-CY (article 46 de la Convention de Budapest).
[20] La préparation de cette note d'orientation fait suite aux conclusions du rapport intitulé « Compétence et accès transfrontalier » (T-CY(2012)3) adopté par le T-CY en décembre 2012. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)3F_transborder_repV31public_7Dec12.pdf

légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Extrait du rapport explicatif :

> 293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des États agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. À cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.
>
> 294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations : d'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne « légalement autorisée » pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par exemple, 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. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article.

2. Interprétation de l'article 32 de la Convention de Budapest par le T-CY

Concernant l'article 32a (accès transfrontalier à des données informatiques accessibles au public ou « données ouvertes »), aucun problème particulier n'a été soulevé et il n'est pour l'instant pas nécessaire que le T-CY donne des orientations supplémentaires.

On considère généralement que les membres des services répressifs peuvent consulter toutes les données accessibles publiquement, et qu'à cette fin ils peuvent s'inscrire ou s'abonner aux services ouverts au public.[21]

Si une partie d'un site web, d'un service ou d'un système du même type est fermée au public alors que le reste est accessible, cette partie n'est pas considérée accessible au sens de l'article 32a.

[21] La législation nationale peut toutefois limiter l'accès à des données publiquement disponibles ou leur utilisation par les services répressifs.

Concernant l'article 32b, on peut envisager les situations caractéristiques suivantes :

- 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 forces de l'ordre ou leur permettre d'y accéder, tel que prévu à l'article.[22]

- Un individu suspecté de trafic de drogues est arrêté dans les règles alors que son courrier électronique est ouvert 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.

Les autres situations ne sont ni autorisées ni exclues.[23]

Concernant l'article 32b (accès transfrontalier avec consentement), le T-CY partage l'analyse suivante :

a. Considérations et garanties générales

L'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques dans le cadre de l'article 14.[24]

[22] Paragraphe 294 du rapport explicatif
[23] Paragraphe 293 du rapport explicatif. Voir aussi l'article 39.3 de la Convention de Budapest.

[24] Article 14 – Champ d'application des mesures procédurales
1Chaque 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.
2Sauf 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.
3a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
B Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:
i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,
cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Comme il a été souligné plus haut, les Parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de primauté du droit, conformément à l'article 15 de la Convention de Budapest.[25]

Les droits des individus et les intérêts des tiers doivent être pris en compte dans l'application de cette mesure.

Par conséquent, la Partie qui perquisitionne un autre Etat partie peut envisager d'informer les autorités compétentes de celui-ci.

b. Concernant les notions de « frontière » et de « lieu »

L'accès transfrontalier consiste à « accéder unilatéralement [c'est-à-dire sans passer par l'entraide judiciaire] aux données informatiques stockées sur le territoire d'une autre Partie ».[26]

Cette mesure ne peut s'appliquer qu'entre Parties.

L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat [partie] », ce qui signifie qu'il peut être utilisé lorsqu'on sait où les données se trouvent.

L'article 32b ne prévoit pas certaines autres situations, par exemple lorsque les données ne sont pas stockées sur le territoire d'une autre Partie ou lorsqu'on n'a pas la certitude de leur lieu de stockage. Une Partie ne peut invoquer l'article 32b pour obtenir la divulgation de données stockées sur son propre territoire.

Selon l'article 32b, d'autres situations « ne sont ni autorisées ni exclues. » Ainsi, lorsqu'on ignore si les données sont stockées dans un autre Etat partie ou lorsqu'on n'en a pas la certitude, les Parties peuvent être amenées à évaluer elles-mêmes la légitimité d'une perquisition ou d'un autre type d'accès, à la lumière de leur droit interne, des principes applicables de droit international ou des considérations liées aux relations internationales.

c. Concernant la notion d'« accès sans autorisation de l'autre Partie »

L'article 32b n'impose pas l'utilisation de l'entraide judiciaire, et la Convention de Budapest n'exige pas que l'autre Partie soit informée. Pour autant, la convention n'exclut pas une telle notification. Les Parties peuvent informer l'autre Partie si elles le jugent utile.

---

[25] Article 15 – Conditions et sauvegardes
1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
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.

[26] Paragraphe 293 du rapport explicatif de la Convention de Budapest

d. Concernant le « consentement »

L'article 32b prévoit que le consentement doit être légal et volontaire, ce qui signifie que la personne qui fournit l'accès aux données ou qui consent à les divulguer ne doit avoir subi ni contrainte ni tromperie.[27]

Selon certaines réglementations nationales, il se peut que les mineurs ou les personnes souffrant de troubles mentaux ou d'autres affections ne puissent donner valablement leur consentement.

Dans la plupart des Etats parties, la coopération dans le cadre d'une enquête pénale requiert un consentement explicite. Par exemple, l'acceptation des conditions générales d'utilisation d'un service en ligne peut être insuffisante à constituer un consentement explicite, même si ces conditions indiquent que les données peuvent être transmises aux autorités judiciaires en cas d'utilisation frauduleuse.

e. Concernant le droit applicable

Dans tous les cas, les services répressifs doivent appliquer les mêmes normes juridiques dans l'application de l'article 32b que dans leur propre pays. Si l'accès aux données ou leur divulgation ne seraient pas autorisés sur le territoire national, il en va de même dans l'application de l'article 32b.

Les parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de la primauté du droit, conformément à l'article 15 de la Convention de Budapest.

f. Concernant la personne autorisée à fournir l'accès ou à divulguer les données

S'agissant de déterminer « qui » est « légalement autorisé » à divulguer des données, cette question peut varier en fonction des circonstances ainsi que de la législation et de la réglementation en vigueur.

Il peut par exemple s'agir d'un particulier donnant accès à sa messagerie électronique ou à d'autres données qu'il a stockées à l'étranger.[28]

Il peut aussi s'agir d'une personne morale.

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. En général, les prestataires de services ne sont que les dépositaires de ces données. Ils n'en ont pas le contrôle ni la propriété et ne sont donc pas dans la capacité de donner un consentement valide. En revanche, les forces de l'ordre pourront bien sûr se procurer les données dans un pays étranger par d'autres moyens, comme l'entraide judiciaire ou les procédures applicables aux situations d'urgence.

g. Demandes internes légalement formulées et article 32b

L'article 32b ne s'applique pas aux injonctions de produire ni à d'autres demandes légalement formulées au sein d'un Etat partie.

[27] Dans certains pays, le fait d'accepter que les poursuites soient abandonnées, ou que la gravité des chefs d'inculpation ou la durée d'une peine de prison soient réduites constitue un consentement légal et volontaire.
[28] Voir l'exemple donné dans le paragraphe 294 du rapport explicatif

h. Concernant la localisation de la personne consentant à fournir l'accès aux données ou à les divulguer

L'hypothèse habituelle est que la personne qui donne l'accès aux données est physiquement présente sur le territoire de la Partie requérante.

Cependant, de multiples situations sont possibles. On peut envisager que la personne physique ou morale se trouve sur le territoire des services répressifs de l'Etat requérant lorsqu'elle consent à divulguer les données ou à y donner effectivement accès ; ou uniquement lorsqu'elle consent à les divulguer mais pas à y donner accès ; ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle accepte de les divulguer et/ou qu'elle y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle accepte de coopérer ou lorsqu'elle donne effectivement accès aux données. S'il s'agit d'une personne morale, (comme une entité privée), elle peut être représentée simultanément sur le territoire des services répressifs requérants, sur le territoire où se trouvent les données, voire dans un pays tiers.

Il faut tenir compte du fait que de nombreuses Parties s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des services répressifs étrangers désirant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale.

3. Déclaration du T-CY

Le T-CY déclare d'un commun accord que la présente note d'orientation reflète une analyse partagée par toutes les Parties quant à l'étendue et aux éléments de l'article 32.

4.2 Mandat provisoire 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[29] 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. 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 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 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. • 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 la T-CY. • 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. 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 charge des frais [30]

[29] http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/t-cy(2013)F25rev_%20rules_v15.pdf
[30] Soumis à la disponibilité de financement.

	• Jusqu'à5 membres supplémentaires avec prise en charge des frais[31] • Membres additionnels du T-CY (Etats parties) à leur propre frais.

[31] Soumis à la disponibilité de financement.