COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/TCY

Strasbourg, le 21 mai 2018

T-CY (2018)16

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

Élaboration d'un 2e Protocole additionnel à la Convention de Budapest sur la cybercriminalité

Guide de discussion pour les consultations avec la société civile, les autorités chargées de la protection des données et l'industrie

Conférence Octopus, 11-13 juillet 2018

Conseil de l'Europe, Strasbourg, France

Participation aux consultations

Les consultations sur l'élaboration d'un 2e Protocole additionnel à la Convention de Budapest se tiendront dans le cadre de la conférence Octopus sur la cybercriminalité qui aura lieu du 11 au 13 juillet 2018, plus précisément le jeudi 12 juillet.

Elles ont pour but de faciliter les échanges de vues entre des représentants du Comité de la Convention sur la cybercriminalité et :

- **des représentants d'organisations de la société civile et de milieux universitaires**
- **des experts de la protection des données**
- **des acteurs industriels (prestataires de services et associations)**

Les parties intéressées sont invitées **à s'inscrire** à la conférence Octopus entre **le 1er mai et le 10 juin 2018.** Il est à noter que l'espace réservé à la conférence est limité. Les parties intéressées peuvent également envoyer **des commentaires écrits** sur les questions soulevées dans ce guide au plus tard **le 25 juin 2018** à l'adresse suivante : nina.lichtner@coe.int.

Le mandat pour l'élaboration d'un projet de 2e Protocole additionnel définit un cadre général d'éléments à examiner. Les dispositions finales du protocole ne sont pas figées et les négociations n'en sont qu'à un stade très préliminaire.

Programme

Élaboration du Protocole

- Vue d'ensemble, procédure et situation actuelle
- Poursuite des consultations avec la société civile, des autorités chargées de la protection des données et des acteurs industriels

Contexte : raison d'être du Protocole, récapitulatif et faits saillants récents

- Cadre de réflexion
- Faits connexes sur le plan international : propositions de l'UE en matière de preuves électroniques, loi des États-Unis d'Amérique sur la surveillance des données stockées dans le cloud (US Cloud Act)

Dispositions visant à améliorer l'efficacité de l'entraide judiciaire

Information et échange de vues sur :

- l'entraide judiciaire dans des situations d'urgence
- l'entraide judiciaire accélérée aux fins d'obtenir des informations sur les abonnés
- la langue utilisée pour les demandes
- les auditions par vidéoconférence/conférence téléphonique des témoins, victimes et experts
- les enquêtes conjointes et les équipes communes d'enquête

Coopération directe avec les prestataires de services dans l'ensemble des juridictions

Discussion sur les options préliminaires pour faire face aux défis :

- les modèles de coopération volontaire
- les injonctions de produire
- la protection des données et d'autres conditions et garanties
- les incidences sur les concepts de compétence

Accès légal aux données stockées dans le « cloud »

Discussion sur les options préliminaires pour faire face aux défis :

- interprétation de la compétence : critère de rattachement à la juridiction compétente
- l'article 32 de la Convention de Budapest
- les options pour délimiter les pratiques
- les conditions et sauvegardes

1 Contexte

L'évolution des technologies de l'information et de la communication offre des possibilités sans précédent pour l'humanité mais pose également un certain nombre de questions, notamment pour la justice pénale et, partant, pour l'état de droit dans le cyberespace. La cybercriminalité et d'autres infractions qui sont susceptibles d'impliquer des preuves électroniques sur les systèmes informatiques se développent à grande vitesse et les éléments de preuve correspondants sont de plus en plus stockés sur des serveurs situés dans des juridictions étrangères, multiples, itinérantes ou inconnues, c'est-à-dire dans le « cloud ». Or les pouvoirs des services de répression dans ce domaine sont généralement limités par les frontières territoriales.

Les Parties à la Convention de Budapest, qui sont représentées au Comité de la Convention sur la cybercriminalité, ont cherché des solutions entre 2012 et 2014 en s'appuyant sur un groupe de travail sur l'accès transfrontalier aux données, et entre 2015 et 2017 par le biais du Groupe sur les preuves dans le cloud.

Suite aux résultats obtenus par ce dernier, le T-CY a adopté les recommandations suivantes :

1. Renforcer l'efficacité du processus d'entraide judiciaire en donnant suite aux recommandations antérieures adoptées par le T-CY en décembre 2014.
2. Élaboration d'une note d'orientation sur l'article 18 de la Convention de Budapest sur les injonctions de produire concernant des informations sur les abonnés.
3. Application intégrale de l'article 18 par les Parties dans leur droit interne.
4. Adoption de mesures concrètes visant à renforcer la coopération avec les prestataires de services.
5. Négociation d'un 2e Protocole additionnel à la Convention de Budapest sur le renforcement de la coopération internationale.

En juin 2017, le T-CY a approuvé le mandat pour l'élaboration du Protocole au cours de la période allant de septembre 2017 à décembre 2019. Les éléments suivants doivent être pris en considération :

A. Dispositions relatives à une entraide judiciaire plus efficace (par exemple l'entraide judiciaire accélérée pour l'obtention d'informations sur les abonnés, les injonctions de produire internationales, les enquêtes conjointes, les procédures d'urgence, etc.).
B. Dispositions permettant de coopérer directement avec des prestataires d'autres juridictions concernant des demandes d'informations sur les abonnés, des demandes de conservation et des demandes urgentes.
C. Un cadre plus clair et des garanties renforcées pour les pratiques actuelles en matière d'accès transfrontalier aux données.
D. Des garanties, notamment des critères en matière de protection des données.

Le mandat pour l'élaboration d'un projet de 2e Protocole additionnel définit un cadre général d'éléments à examiner. Toutefois, les dispositions finales du Protocole ne sont pas figées; la pertinence de chacune des questions et la viabilité des réponses, notamment celles qui sont

examinées aujourd'hui, ainsi que d'autres questions qui pourraient se poser, devront être déterminées pendant la négociation du Protocole.

Le T-CY a décidé de prolonger les séances plénières ordinaires pour la négociation et de créer un « Groupe de rédaction du protocole » qui sera chargé d'élaborer le texte entre les sessions plénières.

Des réunions du Groupe de rédaction du protocole et des sous-groupes correspondants ont eu lieu en septembre 2017, février 2018, avril 2018 et mai 2018, tandis qu'une séance plénière de rédaction du protocole s'est tenue en novembre 2017;une autre est prévue en juillet 2018.

Les participants à ces réunions ont examiné les aspects conceptuels des dispositions à élaborer et ont élaboré un projet de texte visant à améliorer l'efficacité de l'entraide judiciaire (langue des demandes, auditions audio/vidéo, entraide judiciaire en situation d'urgence). On note cependant qu'en mai 2018, les projets n'avaient pas suffisamment évolué pour justifier des consultations avec d'autres parties prenantes.

Avant de procéder à l'élaboration de dispositions plus complexes (telles que la coopération directe avec les prestataires, l'élaboration d'un cadre pour les pratiques d'accès transfrontalier, l'état de droit et les garanties en matière de protection des données), le T-CY souhaite participer à une première série de consultations avec la société civile, des organismes de protection des données et des acteurs industriels.

2 Objectif des consultations

Le Comité de la Convention sur la cybercriminalité (T-CY) souhaite consulter la société civile, les organisations de protection des données et les acteurs industriels pendant le processus de rédaction afin de recueillir leurs avis et de tirer parti de leur expérience.

La conférence Octopus du 11 au 13 juillet 2018 sera l'occasion de mener de telles consultations. Un atelier d'une journée leur sera consacré le jeudi 12 juillet[1]. D'autres réunions seront organisées lorsque les projets de concept et de texte seront disponibles.

3 Questions à examiner

3.1 Contexte : raison d'être du Protocole, récapitulatif et faits saillants récents

Cette session a pour but de récapituler et de confirmer à nouveau les motifs pour lesquels un protocole additionnel à la Convention de Budapest doit être élaboré. Les participants sont également invités à examiner les faits saillants récents et leurs incidences possibles sur les travaux relatifs au Protocole.

▶ **Cadre de réflexion**

- La portée mondiale grandissante de la Convention de Budapest et la nécessité de tenir compte des lois, des exigences et des pratiques de toutes les Parties.

[1] Un autre atelier sur l'accès aux données WHOIS (entrées contenant les informations relatives à l'enregistrement des noms de domaine) aura lieu dans la matinée du 13 juillet.

- Les défis qui se posent à la justice pénale en matière d'accès aux données stockées dans le « cloud ».

- Le champ d'application du Protocole en matière de justice pénale : enquêtes et procédures pénales relatives à la cybercriminalité et aux preuves électroniques (articles 14 et 25.1 de la Convention de Budapest).

- Questions spécifiques à prendre en considération dans l'élaboration du Protocole:
  - la nécessité de faire la distinction entre les informations sur les abonnés, le trafic et le contenu en termes d'exigences et de seuils d'accès à des données pouvant être utiles dans le cadre d'enquêtes criminelles spécifiques ;
  - la divulgation accélérée des informations sur les abonnés ;
  - les cas de « disparition (de la connaissance) du lieu » où se trouvent les données, ou dans lesquels on soupçonne que le lieu de stockage des données se trouve sur le territoire d'un autre État ;
  - le fait que les États recourent de plus en plus à un accès unilatéral transfrontière aux données sans règles internationales claires lorsque l'entraide judiciaire n'est pas possible ;
  - les problèmes que posent, en matière d'entraide judiciaire, la sécurisation et l'obtention des preuves électroniques volatiles émanant d'un autre État, ainsi que les moyens d'améliorer cette entraide ;
  - le système actuel de communication volontaire des données par les prestataires de services américains, les restrictions à la divulgation d'informations par les fournisseurs situés dans d'autres États et les moyens de faciliter les contacts directs entre les services de répression et les prestataires ;
  - la question de la divulgation accélérée des données dans les situations d'urgence ;
  - la nécessité de fournir des garanties et des conditions qui assurent une protection des données mais aussi une protection adéquate des droits de l'homme et des libertés telle qu'elle s'applique aux Parties de nombreux systèmes et cultures juridiques différents.

▶ **Faits saillants au niveau international**

- Localisation des données ou localisation du contrôleur de données ou de la personne en possession ou en contrôle :
  - La territorialité et les questions relatives aux critères de localisation des données ;
  - La question des représentants des contrôleurs ou des responsables du traitement des données (article 27 du Règlement général sur la protection des données), et des représentants des prestataires de services numériques offrant un service au sein de l'UE (considérant 65 et directive sur la sécurité des réseaux et systèmes d'information (NIS), article 18);
- loi des États-Unis d'Amérique sur la surveillance des données stockées dans le cloud (US Cloud Act) ;
- Propositions de l'Union européenne sur les preuves électroniques[2].

[2] Il s'agit notamment de propositions pour une:
- réglementation des injonctions de produire; https://ec.europa.eu/info/sites/info/files/placeholder.pdf
- directive sur le représentant légal; https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf

a Question : Quelles sont les incidences de ces différents faits saillants sur les travaux relatifs au Protocole ?

3.2 Dispositions visant à améliorer l'efficacité de l'entraide judiciaire

La fourniture d'une entraide juridique plus efficace sur la cybercriminalité et les preuves électroniques est une priorité des Parties à la Convention de Budapest. En conséquence, la phase initiale du processus de rédaction s'est concentrée sur les dispositions relatives à cette entraide. Cette session vise à informer les participants des progrès accomplis à cet égard.

▶ **Introduction: Recommandations du T-CY 2014 et suite donnée par les Parties**

▶ **Information et échange de vues sur :**

- l'entraide judiciaire en situations d'urgence ;
- la langue utilisée pour les demandes ;
- les auditions audio/vidéo ;
- les équipes communes d'enquête.

b Question : la société civile, les autorités chargées de la protection des données ou les acteurs industriels ont-ils des avis sur ces propositions ?

3.3 Coopération directe avec les prestataires de services dans l'ensemble des juridictions

Les Parties à la Convention de Budapest – autres que les États-Unis d'Amérique - envoient directement plus de 150 000 demandes par an aux principaux prestataires de services américains qui, dans environ 60 % des cas, communiquent volontairement des informations sur les abonnés aux autorités judiciaires étrangères. Ces prestataires peuvent également communiquer volontairement des données sur le contenu dans des situations d'urgence par l'intermédiaire d'une entité gouvernementale américaine. Les politiques, les pratiques et les taux de réponse des prestataires aux pays varient et suscitent des préoccupations. De même, les prestataires de la plupart des autres pays ne sont pas en mesure de communiquer volontairement des données lorsqu'elles sont directement demandée par des autorités étrangères. Les Parties étudient les propositions initiales en vue de leur inclusion dans le Protocole, notamment :

a) un cadre juridique plus clair entre les Parties définissant les règles de communication volontaire d'informations sur les abonnés – et dans les situations d'urgence également - par des prestataires ;
b) les options concernant la communication obligatoire d'informations sur les abonnés ;
c) les demandes directes de conservation adressées aux prestataires.

Cette session a pour objet de discuter de la viabilité de ces options et de leur compatibilité avec les exigences en matière de protection des données.

▶ **Divulgation volontaire [d'informations sur les abonnés] par les prestataires de services**

- Examen des pratiques actuelles[3].

[3] Voir le rapport final du Groupe de travail du T-CY sur les preuves dans le cloud https://rm.coe.int/168064b77d

- Portée et restrictions de l'article 18 de la Convention de Budapest (voir la note d'orientation sur l'article 18 de la Convention de Budapest relative aux injonctions de production concernant les informations sur les abonnés).

c Questions : les pratiques actuelles des prestataires américains peuvent-elles être transposées et généralisées dans un protocole ?

i. En ce qui concerne les informations sur les abonnés ?
ii. Pour la divulgation d'autres données dans des situations d'urgence ?

d Question : quels sont les règles/règlements ou d'autres facteurs qui empêchent les prestataires de communiquer volontairement des informations sur les abonnés aux autorités de justice pénale d'autres juridictions ?

e Questions : facteurs de rattachement à la juridiction compétente : dans quelles circonstances les prestataires de services peuvent-ils faire l'objet d'une injonction nationale de produire ?

i. « Lien réel et substantiel » à une Partie ?
ii. « Offrant des prestations sur le territoire d'une Partie » ?
iii. « Ou « établi » dans la Partie[4]?

f Questions relatives à la protection des données et d'autres garanties pour la communication volontaire d'informations :

i. Quelle protection des données et autres garanties s'appliquent :
   - Au cadre juridique du pays du prestataire de services ?
   - Au cadre juridique du pays qui soumet une demande à une autorité de justice pénale ?
   - Au cadre juridique du pays où les données sont stockées ?
   - Au cadre juridique du pays de la personne concernée ? Si plusieurs pays sont impliqués ?

ii. De la part du prestataire de services qui est considéré comme le contrôleur de données dans le cadre juridique européen :
   - Quelles conditions doivent être remplies précisément pour permettre la divulgation et quelles sont les dispositions applicables du **Règlement général sur la protection des données** ou de la Convention 108 ?
   - Qu'est-ce qui serait considéré comme une base juridique suffisante au regard du Règlement général sur la protection des données ou de la Convention 108 ?
   - Qu'est-ce qui constitue un « intérêt légitime »[5] (article 6.1. f) du Règlement général sur la protection des données) d'un prestataire de services dans ce contexte ?

[4] Voir la Cour de justice de l'Union européenne à cet égard, en particulier les affaires en lien avec « l'offre d'un service à » ou « l'acheminement d'un service vers » un État membre de l'Union européenne, notamment les affaires C-131/12 (Google Espagne), l'affaire C-230/14 (Weltimmo*) ou* les affaires C-595/08 et C-144/09 (Pammer et Halpenof). Pour une brève présentation de ces affaires, voir le chapitre 3.4 de T-CY(2016)5 https://rm.coe.int/16806a495e

[5] Voir aussi Groupe de l'article 29: Avis 06/2014 sur la notion d'intérêt légitime du contrôleur de données au sens de l'article 7 de la directive 95/46/CE ; http://www.dataprotection.ro/servlet/ViewDocument?id=1086

- Quelles sont les exigences en matière de divulgation/transfert d'informations sur les abonnés à des « pays tiers » ?
- Les dérogations prévues à l'article 49 du Règlement général sur la protection des données (article 49.1 f)) s'appliquent-elles si des données sont demandées dans le cadre d'une enquête pénale spécifique ?
- Quel est le sens de l'article 48 du Règlement général sur la protection des données ?

iii. Dans le pays demandeur (c'est-à-dire dans le pays de destination des données) :
- Quelles conditions précises doivent être remplies pour permettre le transfert vers ce pays et quelles sont les dispositions applicables du **Règlement général sur la protection des données** ou de la Convention 108 ?

iv. Quelles mesures de protection des données et autres garanties doivent être prises pour la divulgation volontaire de données dans d'autres juridictions ?

▶ **Conservation volontaire des données par les prestataires de services**

– Bref examen des pratiques actuelles[6].

g Question : les pratiques actuelles des prestataires de services américains peuvent-elles être transposées et généralisées dans un protocole ?

▶ **Injonctions de production obligatoires**

– Bref aperçu des propositions de la Commission européenne relatives à une injonction européenne de production et de conservation[7] et à la manière dont elle fonctionnerait au sein de l'Union européenne.

h Questions : un tel régime obligatoire pourrait-il être envisagé pour des pays non membres de l'UE ?

i. Pour quel type de données ? Uniquement pour des informations sur les abonnés ?
ii. Quels restrictions et facteurs de rattachement à la juridiction compétente ?
iii. Rôle des autorités compétentes dans le pays qui fait l'objet de la demande ?
iv. Application en cas de non-respect de l'injonction ?
v. Garanties et exigences en matière de protection des données ?

[6] Voir le Rapport final du Groupe de travail du T-CY sur les preuves dans le cloud https://rm.coe.int/168064b77d

[7] Il s'agit notamment de propositions pour une:
- réglementation des injonctions de produire; https://ec.europa.eu/info/sites/info/files/placeholder.pdf
- directive sur le représentant légal; https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf

3.4 Accès légal aux données stockées dans le « cloud »

- Brève discussion sur le problème de la disparition (de la connaissance) du lieu et sur la faisabilité de l'entraide judiciaire.

▶ **Interprétation de la compétence : facteurs de rattachement à la juridiction compétente**

i Question : quels sont les facteurs pertinents qui permettent de déterminer la compétence à appliquer (localisation des données ou de l'équipement sur le territoire d'un État et/ou accès d'une personne sur le territoire d'un État qui a « la possession ou le contrôle » des données) ?

j Question : que signifie « transfrontière »?

▶ **Article 32 de la Convention de Budapest**

- Les restrictions à l'article 32 (voir note d'orientation) ;

k Question : d'autres éclaircissements sont-ils nécessaires sur le champ d'application de l'article 32 ?

▶ **Options**

La note d'orientation relative à l'article 32 donne un exemple d'accès transfrontière :
« 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. »

l Question : quels autres scénarios pourraient être envisagés ?

- Scénarios ?
- Risques ?
- Conditions et sauvegardes ?