COUNCIL OF EUROPE

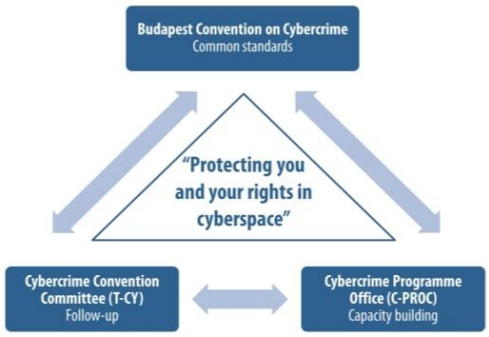
CONSEIL DE L'EUROPE

Version 2 novembre 2017

Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques :

Vers un protocole à la Convention de Budapest

La Convention de Budapest sur la Cybercriminalité a été ouverte à la signature en 2001. Depuis, le nombre des États Parties ne cesse de croître et tout pays en mesure d'en appliquer les dispositions peut demander à y adhérer. Fin octobre 2017, 56 États étaient devenus Parties et 14 autres l'avaient signée ou avaient été invités à y adhérer. La Convention de Budapest est complétée par un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.



La qualité de la mise en œuvre de la Convention de Budapest est évaluée par le Comité de la Convention sur la cybercriminalité (T-CY) représentant les Parties à cette Convention.

Les États qui se sont engagés à coopérer au titre de cette Convention sont en outré aidés pour ce faire grâce à des projets de consolidation de capacités gérés par un Bureau dédié, le Bureau du Conseil de l'Europe pour le Programme sur la cybercriminalité (C-PROC) en Roumanie.

L'évolution des technologies de l'information et de la communication, si elle a ouvert des possibilités inouïes pour l'humanité, pose également des défis, notamment pour la justice pénale et donc pour l'État de droit dans le cyberespace. Alors que prospèrent la cybercriminalité et les autres infractions entraînant des preuves électroniques sur des systèmes informatiques, et que ces preuves sont de plus en plus stockées sur des serveurs hébergés dans des juridictions étrangères, multiples, fluctuantes ou inconnues, autrement dit dans le Cloud, les pouvoirs des services répressifs sont limités par les frontières territoriales.

Les Parties à la Convention de Budapest Convention cherchent depuis quelque temps déjà des solutions dans ce domaine : de 2012 à 2014, un groupe de travail sur l'accès transfrontière aux données a travaillé sur la question, puis de 2015 à 2017, le flambeau a été repris par le Groupe sur les preuves dans le Cloud. Celui-ci a proposé de se concentrer sur les questions spécifiques ci-après :

- la nécessité de poser des exigences et des seuils différents pour l'accès aux données dans des enquêtes pénales spécifiques, selon qu'il s'agit de données concernant l'abonné, le trafic ou le contenu ;
- l'efficacité limitée de l'entraide judiciaire pour sécuriser des preuves électroniques volatiles ;
- les situations de perte de (connaissance de la) localisation des données et le fait que les États recourent de plus en plus à l'accès transfrontalier unilatéral de données en l'absence de règles internationales ;

- la question de savoir à partir de quand la présence ou l'offre de service d'un fournisseur de services sur le territoire d'une Partie est suffisante pour que le fournisseur devienne assujetti aux pouvoirs répressifs de cette Partie ;
- le régime actuel de publication volontaire des données par les fournisseurs américains qui peut aider les services répressifs mais peut aussi se révéler préoccupant ;
- la question de la divulgation accélérée de données en situations d'urgence ;
- la protection des données et autres sauvegardes de l'État de droit.

A la suite des résultats obtenus par le Groupe sur les preuves dans le Cloud, le T-CY a adopté les Recommandations suivantes :

1. renforcer l'efficacité du processus d'entraide mutuelle en appliquant les Recommandations précédentes adoptées par le T-CY en décembre 2014 ;
2. une Note d'orientation sur l'article 18 de la Convention de Budapest concernant les injonctions de produire pour des informations relatives aux abonnés. Cette Note explique comment les injonctions de produire nationales pour des informations relatives aux abonnés peuvent être émises à l'intention d'un fournisseur de services national indépendamment du lieu où se trouvent les données (article 18.1.a) et à l'intention de fournisseurs offrant un service sur le territoire d'une Partie (article 18.1.b) ;
3. la pleine mise en œuvre de l'article 18 par les Parties dans leur droit national ;
4. des mesures concrètes pour renforcer la coopération avec des fournisseurs de services ;
5. la négociation d'un 2e Protocole additionnel à la Convention de Budapest sur une coopération internationale renforcée.

En juin 2017, le T-CY s'est entendu sur un Mandat pour la préparation du Protocole entre septembre 2017 et décembre 2019. Les éléments suivants doivent être pris en compte :

A. des dispositions sur une entraide judiciaire plus efficiente (par exemple une entraide accélérée pour les informations relatives à un abonné, des injonctions de produire internationales, des enquêtes conjointes, des procédures d'urgence etc.) ;
B. des dispositions sur la coopération directe avec des fournisseurs dans d'autres juridictions ;
C. un cadre et des sauvegardes pour les pratiques existantes en matière d'accès transfrontalier aux données ;
D. des sauvegardes pour l'État de droit et la protection des données.

Le T-CY est convenu d'étendre les réunions plénières normales pour la négociation du Protocole et d'établir un "Groupe de rédaction du Protocole" chargé de travailler sur le texte entre les sessions plénières.

43 experts de 28 États Parties ont participé à la première réunion du Groupe de rédaction en septembre 2017. Il a été décidé entre autres :

- d'entamer une étroite consultation avec la société civile, les organisations de protection des données et le secteur du Net durant le processus de rédaction. Des réunions spécifiques seront organisées pour ce faire, une fois que l'on disposera des concepts et du texte pour la rédaction. La Conférence Octopus du 11 au 13 juillet 2018 sera également l'occasion d'un échange de vues ;
- qu'au vu des évolutions au niveau de l'Union européenne concernant la preuve électronique et la justice pénale dans le cyberespace, "il conviendra de rechercher une étroite coordination dans la rédaction du Protocole addition à la Convention de Budapest et pour la préparation des instruments juridiques pertinents par l'Union européenne".

Les problématiques à résoudre sont complexes et il pourrait être difficile de parvenir à un consensus sur les options actuellement sur la table. Cependant, à moins de s'entendre sur des solutions, les gouvernements risquent d'être de moins en moins capables de préserver l'État de droit pour protéger les personnes et leurs droits dans le cyberespace.

Pour de plus amples informations, veuillez contacter :

Le Secrétariat du Comité de la Convention sur la cybercriminalité
Division Cybercriminalité, DGI
Conseil de l'Europe
Strasbourg, France
Email cybercrime@coe.int

www.coe.int/cybercrime