www.coe.int/cybercrime

Strasbourg, 18 mars 2016

« Groupe sur les preuves dans le Cloud » (CEG)

Invitation à un

Echange de vues avec des organisations de protection des données

Lundi 23 mai 2016, 11h00 - 17h00, Salle 5, Palais de l'Europe
Conseil de l'Europe, Strasbourg, France

1 Participation

La réunion est ouverte aux représentants des instances suivantes :

1. T-PD / Conseil de l'Europe
2. Groupe de travail 29
3. Contrôleur européen de la protection des données (CEPD)
4. Commission européenne - DG Justice et DG Affaires intérieures
5. Parlement européen - Commission des libertés civiles, de la justice et des affaires intérieures (LIBE)
6. Etats membres et observateurs de la Convention Cybercriminalité (T-CY)

La réunion se tiendra le 23 mai 2016 11 heures à 17 heures, salle 5, au Palais de l'Europe, Conseil de l'Europe, à Strasbourg (France).

Les représentants doivent s'inscrire à l'avance afin d'obtenir des badges pour accéder au bâtiment.

Pour faciliter et structurer les discussions, les représentants intéressés sont invités à soumettre des contributions écrites traitant des questions énumérées dans la présente note.

Date limite pour l'inscription et les contributions écrites : **1er mai 2016**.

Pour les inscriptions, observations écrites et autres informations, veuillez contacter :

Alexandru FRUNZA,
Responsable de programme
Division de la cybercriminalité
Tél. +33 390215897
Alexandru.FRUNZA@coe.int

2 Contexte

Le Comité de la Convention Cybercriminalité (T-CY), lors de sa 12e réunion plénière (2-3 décembre 2014), a mis en place un groupe de travail pour étudier les solutions concernant l'accès aux éléments de preuve dans le Cloud à des fins de justice pénale, notamment à travers une entraide judiciaire (« Groupe sur les preuves dans le Cloud »).[1]

Cette décision a été motivée par le fait que, compte tenu de la prolifération de la cybercriminalité et autres infractions impliquant des éléments de preuve électroniques, et dans le contexte de l'évolution technologique et de l'incertitude en matière de compétence territoriale, des solutions supplémentaires sont nécessaires pour permettre aux services de justice pénale d'obtenir des preuves électroniques précises dans des enquêtes pénales spécifiques.[2]

Le Groupe sur les preuves dans le Cloud doit présenter un rapport au T-CY avec des options et des recommandations pour toute action future d'ici à la fin 2016.

Le Groupe sur les preuves dans le Cloud a identifié les défis que les autorités de justice pénale devaient relever pour obtenir des preuves électroniques transfrontières[3] et prépare actuellement les solutions envisageables.[4]

En novembre 2015, le Groupe sur les preuves dans le Cloud a tenu une audition avec des fournisseurs de services,[5] et souhaiterait désormais poursuivre les discussions avec les organisations de protection de données.

3 Objectifs

Le Groupe sur les preuves dans le Cloud recherche les points de vue des organisations de protection des données en ce qui concerne la compatibilité des options et solutions potentielles sur l'accès des services de justice pénale aux éléments de preuve dans le Cloud ou dans des Etats étrangers soumis à la réglementation européenne relative à la protection des données.

---

[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 aux données, adopté lors de la 12e réunion plénière du T-CY, décembre 2014).

[2] La nécessité de trouver des solutions permettant un accès en temps opportun aux preuves électroniques en vue de protéger les droits des victimes est également soulignée par l'Union européenne dans le document http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/fr/pdf (février 2015). Le programme européen en matière de sécurité de l'UE (avril 2015) note : « *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 en 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_fr.pdf

Le T-CY dans le document T-CY(2014)16
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf a déclaré :
« 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. »

[3] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b5

[4] Pour un résumé informel des questions actuelles et des options envisagées, voir https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a53c8

[5] http://www.coe.int/en/web/cybercrime/hearing

4 Thèmes pour les discussions

La réunion portera essentiellement sur les questions suivantes :

Question 1:	En décembre 2015, l'Union européenne a conclu un accord sur le fond pour un nouveau Règlement général sur la protection des données et une Directive sur la protection des données en matière pénale. Le Protocole portant amendement à la Convention n° 108 du Conseil de l'Europe sur la protection des données va bientôt être finalisé. Quelles sont les implications de ces instruments eu égard à la Convention de Budapest sur la cybercriminalité sous sa forme actuelle ?
Question 2:	Les autorités judiciaires pénales vont peut-être devoir divulguer des données à caractère personnel directement à un fournisseur de services d'un autre Etat, par exemple, dans des situations de danger imminent ou lorsque d'autres circonstances l'exigent. Cela semble être prévu à l'Article 36aa de la future Directive de l'UE :
a)	Cela change-t-il quelque chose si le fournisseur de services se trouve dans un Etat membre de l'UE, dans un autre Etat partie à la Convention n° 108, ou dans un pays tiers ?
b)	Un Protocole à la Convention de Budapest pourrait-il servir de base juridique à un tel processus? Si oui, quels seraient les éléments à prévoir?
Question 3:	Les autorités de justice pénale envoient de plus en plus de demandes d'informations sur les abonnés (et parfois aussi d'autres données) directement aux fournisseurs de services d'autres Etats, et souvent, ces fournisseurs répondent positivement à cette demande. Dans des situations d'urgence, notamment les situations d'abus commis à l'encontre d'enfants, les fournisseurs de services sont parfois prêts à divulguer aussi des informations relatives au contenu :
a)	Quels seraient la base ou le raisonnement, en vertu des instruments européens de protection des données et/ou des législations nationales, qui permettraient une telle divulgation directement au-delà des frontières dans des situations non urgentes ?
b)	Quels seraient la base ou le raisonnement, en vertu des instruments européens de protection des données et/ou des législations nationales, qui permettraient une telle divulgation, y compris du contenu, directement au-delà des frontières dans des situations d'urgence ?
c)	Cela change-t-il quelque chose si les services de justice pénale qui reçoivent ces informations sont situés dans un État membre de l'UE ou un pays ou territoire approprié, dans un autre Etat partie à la Convention n° 108 ou dans un pays tiers ?
d)	Un Protocole à la Convention de Budapest pourrait-il servir de base juridique à un tel processus? Si oui, quels seraient les éléments à prévoir?
Question 4:	Les fournisseurs de services recevant des demandes de données de la part des services de justice pénale d'un autre pays peuvent le signaler à leurs clients. La notification au client peut nuire aux enquêtes ou aux témoins ou menacer la sécurité des responsables de l'application de la loi ayant déposé une telle demande. La notification des clients est-elle une obligation en vertu

	des instruments de protection des données (par exemple, au titre de l'Article 14 du futur Règlement général sur la protection des données) ?