www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 5 novembre 2013 T-CY (2013)30

Comité de la Convention Cybercriminalité (T-CY)

Groupe ad hoc du T-CY sur l'accès transfrontalier aux données et sur les questions de compétence territoriale

Rapport du Groupe sur l'accès transfontalier 2013

Contents

Contact

Alexander Seger
Secrétaire du Comité de la Convention Cybercriminalité
Chef de la Division Protection des données et cybercriminalité
Direction Générale des droits de l'homme et de l'état de droit
Conseil de l'Europe, Strasbourg, France

Tél. +33-3-9021-4506
Télécopie +33-3-9021-5650
Courriel alexander.seger@coe.int

1 Introduction

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 Comité de la Convention Cybercriminalité (T-CY) lors de la 6e séance plénière (23-24 novembre 2011).

En vertu du mandat adopté par le T-CY, il est chargé :

> d'élaborer un instrument tel qu'un amendement à la Convention, un protocole ou une recommandation visant à mieux réglementer l'accès transfrontalier aux données et aux flux de données, ainsi que le recours aux mesures d'enquêtes transfrontalières sur Internet et les questions y afférentes, et de soumettre cet instrument au Comité dans un rapport présentant ses conclusions.

Le Groupe sur l'accès transfrontalier a présenté un long rapport, intitulé « Compétence et accès transfrontalier : quelles solutions ? »[1], à la 8e séance plénière du T-CY. Ce dernier a adopté le rapport le 6 décembre 2012.

Le 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 afin que ce dernier[2] :

- prépare une note d'orientation sur l'article 32, y compris en consultant des entités du secteur privé ;
- soumette un projet de mandat pour la préparation d'un protocole ;
- prépare un premier projet de protocole pour discussion lors de la 10e séance plénière en décembre 2013.

Le présent rapport résume les travaux menés par le Groupe sur l'accès transfrontalier en 2013 et fait des propositions concernant les prochaines étapes.

[1] Voir l'annexe pour un résumé et les conclusions. Le rapport complet est disponible à l'adresse suivante : http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY%282012%293F_transborder_repV31public_7Dec12.pdf

[2] En 2012, les membres du Groupe transfrontalier étaient les suivants : Ioana Albani (Roumanie), Andrea Candrian (Suisse), Markko Kunnapu (Estonie), Erik Planken (Pays-Bas), Betty Shave (Etats-Unis), Branko Stamenkovic (Serbie) et Pedro Verdelho (Portugal). En 2013, ils ont été rejoints par Tsuyoshi Kitagawa (Japon), Cristina Schulman (Roumanie) et Justin Millar (Royaume-Uni).

2 Activités en 2013

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

En 2013, le Groupe sur l'accès transfrontalier a mené les activités ci-après :

6-7 février 2013, Strasbourg	réunion du Groupe sur l'accès transfrontalier
31 mai – 2 juin 2013, Klingenthal	réunion du Groupe sur l'accès transfrontalier
3 juin 2013, Strasbourg	audition publique
4-5 juin 2013, Strasbourg	séance plénière du T-CY
1-2 octobre 2013, Strasbourg	réunion du Groupe sur l'accès transfrontalier
4 novembre 2013	conférence téléphonique

2.2 Eléments concernant un protocole

Le Groupe sur l'accès transfrontalier a examiné les situations que pourrait couvrir un éventuel protocole à la Convention de Budapest[3] :

- l'accès transfrontalier avec consentement, mais non limité aux données stockées « dans une autre Partie » ;
- l'accès transfrontalier sans consentement, mais par des moyens obtenus légalement ;
- l'accès transfrontalier sans consentement de bonne foi ou dans des situations urgentes
- ou exceptionnelles ;
- l'extension des perquisitions sans restriction au territoire de l'Etat enquêteur ;
- le pouvoir d'utilisation comme critère de légalité des recherches.

Le Groupe sur l'accès transfrontalier réitère ce qu'il a déjà indiqué aux paragraphes 309 et 310 du rapport détaillé adopté en décembre 2012 (T-CY(2012)3) :

> 309 Il sera essentiel de prévoir des garanties et des conditions pour protéger les droits individuels et éviter les abus.
>
> 310 Le fait que les autorités répressives de nombreux Etats procèdent déjà à des accès transfrontaliers aux données au-delà du champ de la Convention de Budapest, sur une base juridique incertaine, avec des risques pour les droits individuels de procédure et de protection de la vie privée et en soulevant des inquiétudes quant à la souveraineté nationale, justifierait qu'on s'engage dans le processus difficile de négociation d'un instrument juridique international contraignant. A l'inverse, en l'absence d'un tel instrument, les risques vont peut-être augmenter.

2.3 Audition publique (3 juin 2013)

Le 3 juin 2013, une audition organisée au Conseil de l'Europe, à Strasbourg, a rassemblé 35 représentants du secteur privé, de la société civile et du monde universitaire et 55 Etats

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf

membres ou observateurs et organisations du T-CY[4]. Un certain nombre de contributions écrites avaient été reçues avant l'audition[5].

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 qui tiennent 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 en matière de consentement volontaire des prestataires de services à divulguer des données.

Cependant, l'audition a également montré que les services répressifs doivent mieux comprendre les règles de protection des données à caractère personnel, tandis que les autorités chargées de la protection des données doivent mieux comprendre les réalités de la cybercriminalité et de la criminalité physique, les preuves électroniques qui s'y rapportent et les mesures légales déjà adoptées dans de nombreux Etats. Il faut également tenir compte du fait que le cadre de la protection des données, qui concerne un grand nombre de Parties, continue d'évoluer aux niveaux du Conseil de l'Europe et de l'Union européenne.

2.4 Note d'orientation sur l'article 32

Le rapport détaillé sur l'accès transfrontalier adopté en décembre 2012 (T-CY(2012)3) contenait déjà, en annexe, les premiers éléments d'une note d'orientation sur l'article 32.

En février 2013, le Groupe sur l'accès transfrontalier a rédigé un projet de note d'orientation[6] en vue de son examen lors de l'audition publique et de la 9e séance plénière du T-CY en juin 2013.

En octobre 2013, il a préparé une version révisée du projet de note d'orientation (voir annexe).

Ce projet, entre autres,

- 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 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 que les services répressifs ne doivent pas invoquer l'article 32b pour prendre des mesures contraires au droit interne ;
- propose 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.

[4] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/PublicHearing_LOP.pdf

[5] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY(2013)PublicHearing_Written_contributions.pdf

[6] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY-2013_7F_GN3_transborder_V2public.pdf

2.5 Décision du T-CY concernant un projet de protocole

Lors de sa 9e séance plénière (4-5 juin 2013), le T-CY a décidé de commencer les travaux sur un projet de 2e Protocole additionnel et a adopté un mandat allant du 1er janvier 2014 au 31 décembre 2015[7].

3 Conclusions et prochaines étapes

Le rapport « Compétence et accès transfrontalier : quelles solutions ? » (T-CY(2012)3) adopté par le T-CY en décembre 2012, les activités menées par le Groupe sur l'accès transfrontalier en 2013 (notamment l'audition publique et les travaux sur le projet de note d'orientation sur l'article 32) et la décision prise par le T-CY le 5 juin 2013 d'entamer la préparation d'un projet de protocole en 2014 ont permis de faire des progrès importants en vue de régler une question qui est considérée comme une « urgence » depuis environ 25 ans. Un certain nombre de points ont été éclaircis.

Les activités menées en 2012/13 ont montré que la nécessité de trouver des solutions était devenue plus pressante. Pendant que les criminels exploitent l'universalité des technologies de l'information et de la communication, les autorités pénales semblent de moins en moins capables de remplir leur obligation positive de protéger la population contre la criminalité, ce qui affaiblit encore l'Etat de droit dans le cyberespace.

Le besoin de solutions reste par conséquent pressant. Cela étant, le Groupe sur l'accès transfrontalier recommande au T-CY d'autoriser une réflexion et un dialogue plus approfondis avec les parties prenantes concernées en 2014, notamment avec le secteur privé et les autorités chargées de la protection des données, et ce pour les motifs suivants :

- les solutions concernant l'accès transfrontalier aux données doivent s'accompagner de garanties et de conditions permettant de protéger les droits des individus et de prévenir les abus, mais il est difficile de concilier l'accès transfrontalier aux données avec ces garanties. L'audition publique du 3 juin a montré qu'une réflexion plus poussée pourrait être nécessaire, ce qui passerait par une poursuite du dialogue entamé au printemps 2013 entre le Groupe sur l'accès transfrontalier et les autorités chargées de la protection des données, la société civile et les organisations du secteur privé ;

- la Convention de Budapest, traité relatif au domaine pénal, couvre des enquêtes ou procédures pénales spécifiques portant sur la cybercriminalité et les preuves électroniques dans le cadre de l'article 14 de la Convention de Budapest. Elle ne s'applique pas aux activités des services chargés de la sécurité nationale. Cependant, le contexte actuel est compliqué et pourrait nuire à la négociation d'un protocole. Dans ce cas, de nombreuses infractions resteraient impunies et les Etats risqueraient d'être dans l'incapacité de remplir leur obligation positive de protéger les individus contre la cybercriminalité ;

- le T-CY réalise actuellement une évaluation de l'article 31 sur l'entraide judiciaire et des autres articles relatifs à la coopération internationale. Il est possible que ce travail débouche sur des propositions supplémentaires à intégrer dans un protocole à la Convention de Budapest.

[7] Voir Annexe 3.3 : http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)22F_PlenAbrMeetRep_V9.pdf.

Au vu de ce qui précède, le Groupe sur l'accès transfrontalier recommande à la séance plénière du T-CY d'autoriser une réflexion et un dialogue plus approfondis avec les parties prenantes concernées et de tenir compte des résultats du cycle d'évaluation mené actuellement par le T-CY.

Cette période pourrait aussi être mise à profit pour approfondir l'examen du projet de note d'orientation sur l'article 32. La véritable négociation d'un projet de protocole ne pourra commencer que lorsqu'un rapport sur les activités susmentionnées aura été remis par le Groupe sur l'accès transfrontalier et examiné par le T-CY.

4 Annexe

4.1 Extraits du rapport du Groupe sur l'accès transfrontalier (décembre 2012)[8]

7 Résumé et conclusions

281 Le Comité de la Convention sur la cybercriminalité (T-CY) a créé lors de sa 6e réunion plénière, en novembre 2011, un « Sous-groupe ad hoc sur la compétence et l'accès transfrontalier aux données et flux de données » (ou « Groupe sur l'accès transfrontalier ») dont le mandat expire le 31 décembre 2012.

282 Le Groupe sur l'accès transfrontalier s'est vu confier la mission suivante :

> élaborer un instrument tel qu'un amendement à la Convention, un protocole ou une recommandation visant à mieux réglementer l'accès transfrontalier aux données et aux flux de données, ainsi que le recours aux mesures d'enquêtes transfrontalières sur Internet et les questions y afférentes, et soumettre cet instrument au Comité dans un rapport présentant ses conclusions.

283 Le Groupe sur l'accès transfrontalier devait examiner en particulier l'application de l'article 32b de la Convention, les pratiques actuelles en matière d'enquêtes transfrontalières et les défis que représentent pour ces enquêtes le droit international sur le ressort territorial et sur la souveraineté des Etats. Le présent rapport reflète les conclusions des travaux menés par le Groupe sur l'accès transfrontalier entre janvier et novembre 2012.

284 Le Groupe sur l'accès transfrontalier estime que deux solutions pourraient être retenues parallèlement, à savoir l'élaboration d'une Note d'orientation du T-CY sur l'article 32 et celle d'un Protocole additionnel sur l'accès aux données. Avant de poursuivre, le Groupe sur l'accès transfrontalier aurait besoin que le T-CY confirme en plénière que ces solutions méritent effectivement d'être retenues. Sous réserve de cette confirmation, il est proposé que le mandat du Groupe sur l'accès transfrontalier soit prolongé jusqu'au 31 décembre 2013.

285 Les conclusions du présent rapport peuvent être résumées comme suit :

Nécessité de l'accès transfrontalier

286 La place grandissant des TIC dans la société s'accompagne d'un accroissement des infractions visant les systèmes informatiques ou commises au moyen de systèmes informatiques. La cybercriminalité porte atteinte aux droits individuels ; les gouvernements ont donc l'obligation positive de protéger la société de ce type de criminalité, entre autres par des mesures de répression appropriées.

287 L'un des premiers objectifs des autorités répressives consiste à recueillir des preuves. Pour la cybercriminalité, mais aussi pour d'autres types d'infractions pénales, elles prennent la forme de preuves électroniques. Les preuves électroniques sont évanescentes et peuvent être stockées sur de multiples territoires. Bien que le principal moyen de recueillir des preuves électroniques stockées dans un autre Etat soit l'entraide judiciaire, l'accès unilatéral aux données peut s'avérer nécessaire dans certaines situations.

[8] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY%282012%293F_transborder_repV31public_7Dec12.pdf

288 La question de l'accès unilatéral, par les autorités répressives d'un Etat, à des données stockées sur un système informatique à l'étranger sans passer par l'entraide judiciaire est débattue depuis les années 1980. Elle est considérée comme urgente depuis le milieu des années 1990. Avec les Principes du G8 sur « l'accès transfrontalier à des données informatiques sans entraide judiciaire », adoptés par les ministres de l'Intérieur et de la Justice à Moscou en 1999, et l'adoption en 2001 de l'article 32 de la Convention de Budapest sur la cybercriminalité, très similaire, un accord a été trouvé sur l'accès transfrontalier dans des circonstances très limitées.

289 Ces dernières années, l'accès transfrontalier est devenu une nécessité de plus en plus impérieuse, compte tenu des points suivants :

- le nombre, la complexité et l'impact des actes de cybercriminalité transnationaux ;
- l'importance de plus en plus grande des preuves électroniques pour tous les types d'infractions pénales ;
- le volume des données et des équipements en circulation, la diversité des services offerts et le nombre de criminels et de victimes sur de multiples territoires ;
- le caractère de plus en plus évanescent des données et des preuves électroniques
- le recours à l'informatique décentralisée et aux services en ligne ;
- la « disparition du lieu », c'est-à-dire la difficulté à rattacher des données – et donc des preuves électroniques – à un territoire ou à un champ de compétence spécifique.

Préoccupations

290 Si les possibilités d'accès transfrontalier devaient s'accroître, il faudrait répondre à plusieurs préoccupations, dont les suivantes :

- des préoccupations juridiques et politiques pour les Etats, notamment concernant le principe de double incrimination ou le refus de coopérer si cela s'avère contraire à leur ordre interne. Ces principes sont pris en compte dans les mécanismes d'entraide judiciaire, mais non nécessairement dans les situations d'accès transfrontalier unilatéral;
- la nécessité de garanties procédurales protégeant les droits des individus dans l'Etat où l'enquête se déroule. Les droits individuels doivent aussi être protégés dans les situations d'accès transfrontalier ;
- les conséquences pour les tiers, notamment les prestataires de services, qui peuvent recevoir des demandes contradictoires de la part de différents Etats ;
- des risques pour la protection des données personnelles. Les prestataires de services et autres entités du secteur privé peuvent enfreindre les règles de protection des données d'un Etat en divulguant des données aux autorités d'un autre Etat[9];
- des risques pour les opérations de police et pour les procédures judiciaires, que l'accès transfrontalier peut venir compromettre.

291 Par conséquent, afin que les Parties se fassent suffisamment confiance pour s'accorder sur un renforcement de l'accès transfrontalier, ce renforcement devrait s'accompagner de garanties et de procédures visant à protéger les droits des individus et des tiers et les intérêts légitimes des

[9] Il convient de noter que les règles de protection des données sont en cours de modification au sein du Conseil de l'Europe et de l'Union européenne. Les travaux à venir sur l'accès transfrontalier devront tenir compte de ces modifications.

autres Etats. Des conditions doivent être mises en place pour empêcher une utilisation abusive de ces pouvoirs.

Dispositions actuelles de la Convention de Budapest

292 En vertu de la Convention de Budapest, le principal moyen d'obtenir des preuves électroniques stockées à l'étranger est l'entraide judiciaire, ou plus précisément une combinaison de mesures provisoires visant à conserver les preuves avant qu'elles ne disparaissent (articles 29 et 30 sur la conservation rapide, article 35 sur le Réseau 24/7) et de demandes formelles de production de ces preuves (en particulier en vertu de l'article 31[10]).

293 L'article 32 est la disposition la plus pertinente concernant l'accès transfrontalier unilatéral. L'accès transfrontalier à des données publiques (article 32a) peut être considéré comme une pratique reconnue sur le plan international, élément du droit coutumier international même au-delà des Parties à la Convention de Budapest.

294 L'article 32b énonce une exception au principe de territorialité en autorisant l'accès transfrontalier unilatéral sans passer par l'entraide judiciaire dans des circonstances limitées. Cette disposition a été formulée de manière à pouvoir englober des scénarios complexes et différents. Elle se limite aux données situées dans des systèmes sur le territoire d'une Partie.

295 Le Groupe sur l'accès transfrontalier ne juge pas nécessaire de modifier l'article 32 sous sa forme actuelle. Cependant, cette disposition étant souvent mal comprise, le T-CY pourrait donner des orientations supplémentaires aux Parties sur des questions comme le sens à donner au « consentement », les lois qui s'appliquent pour définir le « consentement légal » et la personne « légalement autorisée », la personne habilitée à donner accès aux données ou à les divulguer ou le lieu où cette personne est supposée se trouver.

296 L'article 19.2 (perquisition et saisie) permet aux autorités répressives d'étendre un accès ou une perquisition légale du système initial à un système qui lui est connecté, si elles ont des raisons de penser que les données recherchées sont stockées dans un autre système sur leur territoire. Bien que cette mesure ait été conçue comme nationale dans le cadre de la Convention de Budapest, dans le contexte de l'informatique décentralisée, il est souvent difficile de savoir si le système connecté se trouve ou non sur le territoire des autorités répressives. En pratique, il semblerait que la mesure soit donc fréquemment appliquée sans restriction territoriale.

297 L'article 22 établit des principes de compétence généraux et assez larges. La territorialité est le premier principe, mais les principes de pavillon et de nationalité sont également mentionnés et la Convention de Budapest « n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne » (article 22.4). Il semblerait donc que l'article 22 ne constitue pas un obstacle à des solutions supplémentaires.

298 Même si le principe de territorialité restera prédominant, en particulier concernant la compétence qui s'exerce, on peut douter de la possibilité de l'appliquer dans le « cyberespace», fait de données voyageuses, fragmentées, composites ou dupliquées sur plusieurs serveurs relevant de divers ressorts territoriaux. Il n'est pas possible d'appliquer le principe de territorialité en l'absence de certitude quant à l'emplacement des données.

[10] Il semble que le potentiel de ces dispositions n'ait pas encore été pleinement exploité. Le T-CY, en novembre 2011, a décidé d'évaluer la mise en oeuvre des articles 16, 17, 29 et 30 (sur la conservation rapide) en 2012, et d'entreprendre en 2013 une évaluation des dispositions en matière de coopération internationale (en particulier l'article 31).

299 L'article 32 formule une exception au principe de territorialité puisqu'il prévoit l'exercice d'une compétence sur un territoire étranger, c'est-à-dire l'accès à des données qui sont techniquement stockées sur le territoire d'une autre Partie.

300 Les auteurs de la Convention de Budapest ne considéraient pas l'article 32 comme une panacée, jugeant que les situations non prévues par cet article n'étaient « ni autorisées ni exclues » et que des solutions supplémentaires pouvaient être adoptées à une étape ultérieure108[11].

Pratiques109[12]

301 Les informations disponibles suggèrent que les autorités répressives accèdent de plus en plus à des données stockées dans des ordinateurs à l'étranger pour trouver des preuves électroniques. Ces pratiques peuvent aller au-delà des possibilités restreintes prévues à l'article 32b (accès transfrontalier avec consentement) et dans la Convention de Budapest en général :

- L'article 32b n'est pas très souvent utilisé par les autorités répressives pour accéder à des données stockées dans une autre Partie. Il est peut-être utilisé plus fréquemment pour consulter ou demander des données en possession de prestataires de services ou d'autres entités du secteur privé, telles que des données de trafic ou d'inscription, mais généralement pas des données de contenu générées par des usagers ou des clients. Il n'est pas toujours facile de savoir si une telle mesure est considérée comme une mesure transfrontalière au sens de l'article 32b ou comme une demande nationale, si l'entité en question fournit un service dans le pays des autorités en charge de l'enquête.

- Les autorités répressives peuvent aussi accéder directement à des données en élargissant une perquisition légale d'un système initial à un système qui lui est connecté. D'une certaine manière, l'article 19.2 est appliqué sans restriction au territoire des enquêteurs.

- Souvent, l'accès transfrontalier n'est pas délibéré. Les autorités répressives peuvent agir de bonne foi et ignorer ou ne pas avoir la certitude qu'elles perquisitionnent des données stockées sur un système à l'étranger ; il peut arriver aussi qu'elles ignorent de quel ressort territorial les données relèvent exactement.

- Dans certains Etats et en fonction de la situation précise, une fois que les autorités répressives savent que les données recherchées sont stockées à l'étranger, eles doivent interrompre les recherches, ne sont autorisées qu'à conserver une copie des données ou doivent en avertir l'autre Etat.

- Dans les Etats qui autorisent l'accès transfrontalier, seules les techniques d'enquête les moins intrusives sont permises, telles que l'accès avec consentement ou au moyen de données d'inscription obtenues légalement ou la conservation d'une copie des preuves, tandis que les techniques plus intrusives comme le piratage d'un compte ou d'un système, l'installation d'enregistreurs de frappe permettant une surveillance continue,

[11] Rapport explicatif de la Convention de Budapest, paragraphe 293.
[12] Le Groupe sur l'accès transfrontalier ne s'est intéressé qu'à l'accès aux données à des fins de justice pénale. Ces observations portent donc sur des enquêtes pénales et ne couvrent pas l'accès transfrontalier direct par les pouvoirs publics, ni l'accès à des données via des entités du secteur privé à des fins de renseignement ou de sûreté nationale.

la suppression de données ou la désactivation d'un système peuvent être interdites ou uniquement autorisées dans des circonstances limitées.

- De plus en plus, l'accès aux données stockées à l'étranger est obtenu via des prestataires de services ou d'autres entités du secteur privé, par consentement volontaire ou au travers de mandats judiciaires.

- Les entités privées actives dans plusieurs pays peuvent se heurter à des exigences contradictoires : en répondant à une demande légalement formulée par un Etat, elles peuvent violer les règles de protection de la vie privée ou d'autres législations d'un autre Etat. L'accès transfrontalier aux données et l'utilisation des preuves ainsi obtenues dans une procédure pénale sont habituellement soumis à des conditions et garanties définies par l'Etat enquêteur.

302 Dans l'ensemble, les pratiques, les procédures et les conditions et garanties qui les accompagnent varient considérablement d'un Etat à l'autre. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données personnelles, la base juridique de l'accès aux données stockées à l'étranger ou « quelque part en ligne » ainsi que le principe de la souveraineté nationale.

Solutions proposées

Application plus efficace de la Convention de Budapest

303 La Convention de Budapest est un traité international qui reflète un accord entre les Parties sur les modalités de coopération entre elles. Elle est déjà en vigueur et le nombre de Partie est en augmentation. La Convention, sous sa forme actuelle, couvre une bonne part des besoins des autorités répressives en matière de cybercriminalité et de preuves électroniques. Elle permet aux gouvernements de respecter leur obligation positive de protéger les personnes et leurs droits. S'agissant de la coopération internationale, elle associe l'entraide judiciaire formelle à des mesures provisoires rapides visant à établir des preuves électroniques. Le potentiel de ce traité n'a pas encore été pleinement exploité par toutes les Parties.

304 Les Parties devraient utiliser efficacement la Convention de Budapest sur la cybercriminalité, et notamment ses dispositions en matière de coopération internationale. Les Parties sont invitées à prendre part aux évaluations de certains articles menées à bien par le Comité de la Convention sur la cybercriminalité (T-CY) et à donner suite aux recommandations formulées. Enfin, il serait souhaitable que davantage d'Etats adhèrent à la Convention de Budapest.

Note d'orientation du T-CY sur l'article 32

305 Le T-CY devrait préparer une Note d'orientation sur l'article 32b afin d'aider les Parties à appliquer la Convention de Budapest, de corriger les malentendus concernant l'accès transfrontalier en vertu de cette Convention et de rassurer les tiers.

306 L'article 32b suppose de plus en plus la coopération d'entités du secteur privé. Il sera donc nécessaire de consulter des entités privées et des experts de la protection des données au cours de l'élaboration de la Note d'orientation.

Protocole additionnel sur l'accès aux preuves électroniques

307 Même si la priorité devrait aller à l'application efficace de la Convention de Budapest sous sa forme actuelle, et bien qu'une Note d'orientation du T-CY représente un moyen pragmatique d'en faciliter la mise en oeuvre, des mesures supplémentaires seraient peut-être à envisager, notamment pour tenir compte des cas où les données passent d'un territoire à l'autre ou sont stockées sur des territoires multiples ainsi que des cas où l'emplacement physique des données n'est pas connu. Ces mesures pourraient figurer dans un Protocole additionnel à la Convention de Budapest.

308 Ce Protocole additionnel pourrait couvrir des situations possibles entre Parties à travers différents instruments, comme par exemple :

- l'accès transfrontalier avec consentement, mais non limité aux données stockées dans une autre Partie ;
- l'accès transfrontalier sans consentement mais par des moyens obtenus légalement ;
- l'accès transfrontalier sans consentement de bonne foi ou dans des situations urgentes ou exceptionnelles ;
- l'extension des perquisitions sans restriction au territoire de l'Etat enquêteur ;
- le pouvoir d'utilisation comme critère de légalité des recherches.

309 Il sera essentiel de prévoir des garanties et des conditions pour protéger les droits individuels et éviter les abus. Le fait que les autorités répressives de nombreux Etats procèdent déjà à des accès transfrontaliers aux données au-delà du champ de la Convention de Budapest, sur une base juridique incertaine, avec des risques pour les droits individuels de procédure et de protection de la vie privée et en soulevant des inquiétudes quant à la souveraineté nationale, justifierait qu'on s'engage dans le processus difficile de négociation d'un instrument juridique international contraignant. A l'inverse, en l'absence d'un tel instrument, les risques vont peut-être augmenter.

Prochaines étapes

310 Le T-CY a adopté le présent rapport lors de sa 8e réunion plénière (5-6 décembre 2012) et a décidé de le rendre public.

311 Il a été decidé de prolonger le mandat du Groupe sur l'accès transfrontalier jusqu'au 31 décembre 2013, avec les missions suivantes :

- préparer une Note d'orientation sur l'article 32 de la Convention de Budapest, y compris en consultant des entités du secteur privé. Un projet de texte devrait être préparé pour discussion lors de la 9e réunion plénière du T-CY, mi-2013, et des représentants du secteur privé pourraient être auditionnés à cette occasion. La Note d'orientation serait ensuite présentée pour adoption à la 10e réunion plénière, avant le 31 décembre 2013 ;
- soumettre à l'approbation du T-CY (procédure écrite), pour juin 2013, un projet de mandat par lequel le Comité des Ministres chargerait le T-CY de préparer un Protocole additionnel. Le Groupe devrait à ce stade fournir d'autres éléments concernant le contenu et le champ d'un tel Protocole110 ;
- dans l'attente du mandat du Comité d'experts, préparer un premier projet de Protocole pour discussion lors de la 10e réunion plénière du T-CY, avant le 31 décembre 2013.

312 Le T-CY a décidé d'inviter le Japon à désigner un expert à joindre le Groupe sur l'accès

transfrontalier et d'ouvrir le travail du Groupe aux représentants des autres Parties à la Convention Le projet de mandat serait ensuite soumis pour approbation au Comité des Ministres via le Comité européen pour les problèmes criminels (CDPC).

_____

4.2 Proposition de note d'orientation sur l'article 32

Voir Document T-CY(2013)7 (version du 5 novembre 2013)