www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, version 5 novembre 2013 T-CY (2013)7 E

## Comité de la Convention Cybercriminalité(T-CY)

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

Proposition établie par le Bureau pour examen par le T-CY

Les observations sur ce projet de note d'orientation sont à envoyer à:

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

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.[1]

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.[2]

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.

# 2 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

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[2] 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

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 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.

# 3 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.[3]

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

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.

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.[4]

- 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.[5]

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

### 3.1 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.[6]

---

[4] Paragraphe 294 du rapport explicatif

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

[6] 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,

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.[7]

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.

### 3.2 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 ».[8]

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

---

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.

[7] 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.

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

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.

### 3.3 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.

### 3.4 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.[9]

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.

### 3.5 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.

### 3.6 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.[10]

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

Il est très peu probable que les prestataires de services remplissent les conditions d'un consentement valide et volontaire concernant la divulgation des données de leurs utilisateurs

[9] 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.
[10] Voir l'exemple donné dans le paragraphe 294 du rapport explicatif

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.

### 3.7 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.

### 3.8 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.

## 4 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.