www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 19 février 2013 (projet pour examen) T-CY (2013) 7 F

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

Note d'orientation n° 3 du T-CY
Accès transfrontalier aux données (article 32)

Proposition établie par le Bureau
pour observations par les membres et les observateurs du T-CY
et pour examen lors de la 9e réunion plénière du T-CY (juin 2013)

Contact

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

Tél. +33-3-9021-4506
Fax +33-3-9021-5650
E-mail alexander.seger@coe.int

1 Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies[1].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à l'accès transfrontalier aux données en vertu de l'article 32 de la Convention[2]. Dans l'ensemble, les pratiques, les procédures et les conditions et garanties qui les accompagnent varient considérablement d'un Etat partie 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 « dans le nuage » ainsi que le principe de la souveraineté nationale.

La présente 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 le potentiel de ce traité en matière d'accès transfrontalier aux données.

2 Article 32 de la Convention de Budapest

Texte de la disposition :

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

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 Etats 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

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

[2] L'élaboration de cette note d'orientation fait suite aux conclusions du rapport « Compétence et accès transfrontalier : quelles solutions ? », adopté par le T-CY lors de sa réunion plénière en décembre 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

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. A 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

S'agissant de l'article 32a (accès transfrontalier à des données informatiques stockées accessibles au public (source ouverte)), aucun problème particulier n'a été soulevé et il n'est pour l'instant pas nécessaire que le T-CY donne des orientations supplémentaires.

Il est admis que les autorités répressives peuvent consulter des données publiquement accessibles, si nécessaire en s'enregistrant ou en s'inscrivant à des services mis à la disposition du public[3].

Si une partie d'un site internet ou d'un service en ligne est fermée au public, elle n'est pas considérée comme accessible au public au sens de l'article 32a.

Les autres situations ne sont ni autorisées ni exclues.

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

3.1 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[4] ».

Cette mesure ne peut s'appliquer qu'entre Parties.

[3] Le droit interne, cependant, peut poser des limites à la consultation ou à l'utilisation de données publiques par les autorités répressives.

[4] Rapport explicatif de la Convention de Budapest, paragraphe 293.

L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat ». Cela signifie que l'article 32b peut être utilisé lorsqu'on sait où les données se trouvent.

L'article 32b ne s'applique pas lors les données ne sont pas stockées dans une autre Partie ou lorsque leur emplacement est incertain.

Etant donné que d'autres situations ne sont « ni autorisées ni exclues », lorsqu'on ignore si les données sont stockées dans une autre Partie ou lorsqu'on n'en a pas la certitude, les Etats peuvent être amenés à évaluer eux-mêmes la légitimité d'une perquisition ou d'un autre type d'accès à la lumière de leur droit interne, des principes applicables de droit international ou de considérations liées aux relations internationales.

3.2 Concernant la notion d'« accès sans l'autorisation d'une autre Partie »

L'article 32b n'oblige pas à recourir à l'entraide judiciaire, et la Convention de Budapest ne demande pas que l'autre Partie soit avertie. Dans le même temps, la Convention n'exclut pas non plus une telle notification. Les Parties peuvent avertir l'autre Partie si elles le jugent utile.

3.3 Concernant la notion de « consentement »

L'article 32b prévoit que le consentement doit être légal et volontaire, ce qui signifie que la personne qui fournit l'accès ou consent à divulguer les données ne doit avoir été ni contrainte ni dupée. Les éléments constitutifs du consentement doivent être définis par le droit interne de la Partie à qui le consentement est donné, c'est-à-dire de la Partie qui demande l'accès transfrontalier.

Selon certaines réglementations nationales, il se peut que le consentement ne puisse pas être donné par un mineur ou par des personnes se trouvant dans certaines situations (troubles mentaux par exemple).

Dans la plupart des Parties, la coopération dans le cadre d'une enquête pénale demande un consentement exprès. Par exemple, le fait qu'une personne ait accepté les conditions d'utilisation générales d'un service en ligne ne constitue pas un consentement exprès, même si ces conditions indiquent que les données peuvent être transmises aux autorités pénales en cas d'abus.

3.4 Concernant le droit applicable

S'agissant du « consentement légal » et de la personne « légalement autorisée » à divulguer des données, « légal » désigne pour des raisons pratiques le droit de la Partie qui perquisitionne, puisque les autorités répressives agissent normalement sur la base du droit de leur propre pays. En cas d'accès transfrontalier urgent, il ne serait pas réaliste de demander aux enquêteurs de vérifier les règles applicables à l'utilisation des données dans l'autre Partie.

Les Parties à la Convention de Budapest sont supposées se faire confiance et respecter, conformément à l'article 15 de la Convention, les principes des droits de l'homme et de la prééminence du droit.

3.5 Concernant la personne autorisée à fournir l'accès ou à divulguer les données

S'agissant de savoir « qui » est « légalement autorisé » à divulguer les données, la réponse peut varier en fonction des circonstances et des lois et réglementations applicables.

Par exemple, il peut s'agir d'un particulier donnant accès à sa messagerie électronique ou à d'autres données qu'il a stockées à l'étranger[5].

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

La personne fournissant l'accès peut aussi être un prestataire de services internet ou de services en nuage ou une autre entité privée, si les conditions d'utilisation du service le permettent.

3.6 Concernant le lieu où se trouve la personne qui accepte de fournir l'accès ou de divulguer les données

L'hypothèse de base est que la personne qui fournit l'accès est physiquement présente sur le territoire de la Partie requérante. Dans ce cas, cette personne relève du ressort et des lois de l'Etat enquêteur.

Cependant, de multiples situations sont possibles. On peut imaginer que la personne physique ou morale se trouve sur le territoire des autorités répressives requérantes lorsqu'elle consent à divulguer les données ou lorsqu'elle y donne effectivement accès, ou uniquement lorsqu'elle consent mais non lorsqu'elle donne l'accès, ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle consent à divulguer les données et/ou y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle consent à coopérer ou lorsqu'elle fournit effectivement l'accès. S'il s'agit d'une personne morale (comme une entité privée), elle peut être représentée sur le territoire de l'autorité répressive requérante ou sur le territoire où se trouvent les données, voire en même temps dans un pays tiers.

Il faut tenir compte du fait que beaucoup de Parties s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des autorités répressives étrangères recherchant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale.

3.7 Considérations et garanties générales

L'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques, au sens de l'article 14[6].

---

[5] Voir l'exemple donné au paragraphe 294 du Rapport explicatif.

[6] Article 14 – Portée d'application des mesures du droit de procédure

1. Chaque 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.

2. Sauf 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.

3. a) 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

Comme souligné ci-dessus, les Parties à la Convention de Budapest sont supposées se faire confiance et respecter, conformément à l'article 15 de la Convention, les principes des droits de l'homme et de la prééminence du droit[7].

Les mesures doivent être appliquées en tenant compte des droits individuels et des intérêts des tiers.

Par conséquent, l'Etat perquisitionneur devrait envisager d'avertir les autorités compétentes de l'Etat perquisitionné.

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.

_____

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, 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 de cette section sur les droits, responsabilités et intérêts légitimes des tiers.