Groupe de travail du T-CY Preuves dans le Cloud

Accès de la justice pénale aux preuves électroniques dans le Cloud – Synthèse informelle des problématiques et options à l'examen par le Groupe de travail Preuves dans le Cloud[1]

Contexte

Le Gouvernement est tenu de protéger la société et les individus contre le crime, tout en respectant les normes de l'Etat de droit et des droits de l'homme. Pour la justice pénale, il est essentiel de sécuriser les preuves présentes sur des systèmes informatiques, que ces preuves concernent des infractions relevant de la cybercriminalité ou n'importe quel autre crime ou délit.

Les difficultés auxquelles sont confrontées les autorités de justice pénale ont été identifiées[2]. Il importe maintenant de se concentrer sur des problématiques spécifiques restant à résoudre et de commencer à dégager pour cela des options et des solutions.

Ces solutions vont de mesures permettant de rendre l'entraide judiciaire plus efficiente à une coopération transfrontière directe avec les fournisseurs de services sur internet et à un accès transfrontière direct aux données lorsqu'une entraide judiciaire n'est pas possible ; et ces solutions doivent respecter les conditions imposées pour la protection des données et l'Etat de droit.

Il est nécessaire de poursuivre à la fois des mesures immédiates (comme par exemple une meilleure utilisation des instruments existants, des solutions pragmatiques reposant sur l'expérience acquise ou sur des outils en ligne) et de négocier des solutions juridiques internationales supplémentaires.

Le Groupe de travail Preuves dans le Cloud, du Comité de la Convention sur la cybercriminalité (T-CY) analyse actuellement les problématiques et options ci-dessous.

Problèmes à traiter

Faire la distinction entre trois catégories de données que l'on souhaite obtenir, à savoir les informations sur l'abonné, les données relatives au trafic ou les données relatives au contenu

- Ce dont on a le plus souvent besoin dans les enquêtes criminelles, ce sont les « informations relatives à l'abonné » ; ensuite viennent les données sur le trafic et enfin les données relatives au contenu. Il est donc crucial de traiter le problème de l'obtention des informations relatives à l'abonné.

- La récupération d'informations relatives à l'abonné constitue une ingérence moins lourde dans les droits individuels que l'obtention de données sur le trafic - voire, pire, sur le contenu. Or, le droit interne des différents pays concernant l'accès aux preuves ne reflète pas toujours cet état de fait. Dans certains Etats, les conditions posées à l'accès de la justice

[1] http://www.coe.int/en/web/cybercrime/ceg
[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

pénale aux informations relatives aux abonnés sont relativement peu exigeantes, alors que, dans d'autres juridictions, une injonction des tribunaux peut être exigée. Ces divergences affectent les enquêtes dans le pays comme la coopération internationale, et c'est pourquoi il convient d'harmoniser davantage les règles dans ce domaine[3].

- Ces informations sont en général détenues par des fournisseurs de services du secteur privé et sont obtenues principalement sur injonction de produire, un mode d'opération moins intrusif dans les droits individuels et les intérêts de tiers que la perquisition et la saisie de systèmes informatiques ou l'interception de communications[4].

Entraide judiciaire (MLA)

- Lorsque des preuves électroniques sont stockées dans des juridictions étrangères, l'entraide judiciaire en matière pénale constitue le principal moyen de les obtenir. Il convient de rendre le processus de MLA plus efficient, étant donné la portée des requêtes concernant des preuves électroniques et la volatilité de ces dernières[5].

Impossibilité de déterminer un lieu

- L'entraide judiciaire ne peut pas toujours être activée. Dans des situations spécifiques, par exemple lorsqu'on ne connaît pas l'origine d'une attaque, que des serveurs situés dans plusieurs juridictions sont impliqués ou autre situation caractérisée par une impossibilité de déterminer un lieu et pour lesquelles le principe de territorialité ne peut pas s'appliquer, il faut trouver des solutions, passant notamment par un accès transfrontière aux données dans des enquêtes criminelles spécifiques[2].

- Les conditions et protections en matière d'accès transfrontière aux données dans des enquêtes criminelles spécifiques doivent être définies.

- Faute de solutions internationales, les gouvernements explorent de plus en plus des solutions unilatérales, ce qui crée des risques pour les relations entre Etats et les droits individuels. Une solution internationale commune est nécessaire pour fournir un cadre permettant un accès transfrontière aux données dans des conditions respectueuses du droit.

Fournisseur de service offrant un service sur le territoire d'un Etat

- Souvent, les preuves électroniques – que ce soit les informations sur les abonnés, les données relatives au trafic ou celles relatives au contenu – sont détenues par des fournisseurs proposant divers types de services et stockant des données dans différentes juridictions. Il convient de clarifier si un fournisseur est véritablement présent dans un Etat ou s'il « propose un service sur le territoire » d'un Etat auquel cas il faudra une injonction nationale ou un autre type d'ordonnance coercitive. Cela permettra de mieux définir quel est le droit applicable et quelle juridiction est compétence pour l'exécution.

- En outre, si des informations relatives à l'abonné peuvent être obtenues légalement par le biais d'injonctions nationales, cela permettra de réduire considérablement la nécessité d'une coopération internationale et donc la pression sur le mécanisme d'entraide judiciaire.

[3] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1
[4] Voir article 18 Convention de Budapest.
[5] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

Divulgation « volontaire » par des entités du secteur privé à des autorités de justice pénale dans des juridictions étrangères

- Certains fournisseurs de services – en particulier basés aux Etats-Unis – peuvent répondre directement à des requêtes juridiquement fondées déposées par des autorités de justice pénale d'autres juridictions où ils prêtent des services en vue d'obtenir des informations relatives à l'abonné et des données relatives au trafic. Dans ce cas, les fournisseurs de services évaluent eux-mêmes la licéité de la requête ou la légitimité de la demande et s'il convient donc de conserver des données ou de communiquer volontairement des données relatives au trafic ou à l'abonné. Ils peuvent également notifier leur client de la requête, ce qui risque de compromettre une enquête criminelle. Le nombre de requête directement adressées à des fournisseurs de services dans des juridictions étrangères est certes important, toutefois les politiques des fournisseurs, et donc la coopération, sont évolutives et imprévisibles. Un cadre plus stable est nécessaire.

- Le modèle de coopération volontaire soulève des problèmes en ce qui concerne la protection des données et les exigences de confidentialité, c'est pourquoi les fournisseurs européens choisissent normalement de ne pas divulguer de données directement aux autorités de justice pénale dans des juridictions étrangères, quand bien même la situation serait urgente. Il convient d'identifier des solutions pour veiller à ce que la divulgation respecte les dispositions relatives à la protection des données et à la confidentialité.

- Dans certains pays, les données reçues directement de fournisseurs établis dans des juridictions étrangères ne sont pas recevables comme preuve dans des procédures pénales. Cet obstacle devrait être traité par des réformes des droits internes.

Procédures d'urgence

- Lorsque certaines situations l'exigent, il faudrait disposer de moyens d'action rapide en vue de prévenir un danger imminent pour la vie et la sécurité publique, en d'autres termes des procédures d'urgence permettant d'obtenir des preuves électroniques stockées dans des juridictions étrangères, par le biais de l'entraide judiciaire.

- Dans ce type de circonstances, il faudrait que des procédures d'urgences soient aussi prévues pour obtenir des preuves électroniques directement du fournisseur de services dans une juridiction étrangère.

Protection des données et autres mesures de sauvegarde

- L'accès aux données personnelles dans le cadre du droit de la procédure pénale constitue une dérogation légitime aux conditions applicables en matière de protection des données. Le partage international de données personnelles entre autorités publiques compétentes – comme les autorités de justice pénale – devrait se conformer aux exigences en matière de protection des données s'il est fondé sur des accords de coopération bi- ou multilatérale. Le processus d'entraide judiciaire est conçu pour garantir le respect des dispositions de l'Etat de droit et la protection des droits individuels, en particulier si les données demandées doivent être utilisées comme preuve dans une procédure pénale.

- Toutefois, il n'est pas toujours possible d'activer la MLA. Le partage « asymétrique » de données transfrontière directement entre entités du secteur public et du secteur privé est en augmentation.

- Il existe des instruments européens et internationaux de protection des données couvrant les transferts de données transfrontière, soit d'une entité du secteur privé à une autre entité du secteur privé, soit d'une autorité de justice pénale compétente à une autre autorité de justice pénale compétente. Certains instruments autorisent les transferts asymétriques de données transfrontière d'une autorité de justice pénale compétente d'un Etat à une entité du secteur privé dans un autre Etat, en cas de circonstances exceptionnelles.

- Les instruments actuels de protection des données ne semblent pas avoir prévu spécifiquement des situations où des fournisseurs de services – ou autres entités du secteur privé – sont disposées à divulguer des données transfrontières directement à une autorité de justice pénale dans un autre Etat. Les fournisseurs de services doivent donc évaluer par eux-mêmes si la condition de licéité est remplie et si la requête sert l'intérêt public ou l'intérêt légitime du fournisseur en tant que contrôleur des données. Les fournisseurs peuvent courir le risque de voir leur responsabilité engagée. Il serait bon de mettre en place un cadre plus clair pour la divulgation de données transfrontières du privé vers le public, avec des conditions et des mesures de sauvegarde. Cela aiderait les fournisseurs de services à éviter des situations de conflits entre obligations juridiques.

Options

1. **Mesures juridiques et pratiques au niveau national pour rendre l'entraide judiciaire plus efficiente**

- Au nombre de ces mesures figure la mise en œuvre des recommandations du rapport d'évaluation du T-CY sur le fonctionnement des dispositions relatives à l'entraide judiciaire prévues dans la Convention de Budapest adoptée en décembre 2014[6]. Les 15 premières incombent aux Parties et n'exigent pas de nouvelles normes internationales ; elles devraient donc être mises en œuvre sans délai.

- La recommandation 8, qui concerne les procédures d'urgence, prévoit que les Parties sont encouragées à établir des procédures d'urgence pour les requêtes liées à un risque pour la vie ou à des circonstances similaires qui l'exigent. Le T-CY devrait documenter les pratiques suivies par les Parties et les fournisseurs de services. Les Parties – et le T-CY – devraient lui porter une attention particulière. Il se peut qu'il faille, au besoin, prévoir dans le Protocole à la Convention de Budapest des dispositions relatives à des procédures d'urgence.

- Les Etats devraient faciliter l'accès aux informations relatives à l'abonné dans leur droit interne en faisant la distinction entre données relatives au trafic et informations relatives à l'abonné, ce qui leur permettrait de mettre pleinement en œuvre l'article 18 de la Convention de Budapest.

2. **Note d'orientation sur l'article 18 de la Convention de Budapest concernant l'obtention d'informations relatives à l'abonné et précisions sur les cas où un fournisseur de services relève de la juridiction d'une autorité de justice pénale**

- Une telle Note d'orientation aiderait les Etats à faire un meilleur usage des injonctions enjoignant aux fournisseurs de service de produire des informations relatives à un abonné en vertu de l'article 18 de la Convention de Budapest. Il s'agit là d'une mesure de niveau

6 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

national qui n'exige donc pas d'entraide judiciaire. S'il était fait un meilleur usage de cette disposition, nous aurions là un moyen efficient et légal d'obtenir le type d'informations le plus fréquemment nécessaire dans une enquête criminelle.

3. Mesures pratiques pour faciliter la coopération transfrontière entre les fournisseurs de services et les autorités de justice pénale

- En attendant des solutions à plus long terme, des mesures pratiques (par exemple bâtir des capacités, partager des bonnes pratiques, diffuser en ligne des politiques de fournisseurs et des règles de procédures dans les Etats parties) pourraient être prises pour faciliter une coopération plus cohérente entre les fournisseurs de service et les autorités de justice pénale, en particulier pour ce qui est de la divulgation d'informations relatives à l'abonné sur requête légale dans une enquête criminelle donnée mais aussi en cas d'urgence, et en se référant aux intérêts légitimes et aux exigences en matière de protection des données.

4. **Protocole à la Convention de Budapest**

- Dispositions concernant des options supplémentaires pour une entraide judiciaire plus efficace, notamment :

  - Injonctions de produire internationales (Rec 20 du Rapport d'évaluation du T-CY) ou régime simplifié d'entraide judiciaire pour les informations sur l'abonné
  - Coopération directe entre les autorités judiciaires en matière de requêtes de MLA (Rec 21 du Rapport d'évaluation du T-CY)
  - Enquêtes conjointes et équipes communes d'enquête (Rec 23 du Rapport d'évaluation du T-CY)
  - Requêtes en anglais (Rec 24 du Rapport d'évaluation du T-CY)
  - Auditions audio-/vidéo des témoins et victimes
  - Procédures d'urgence (Rec 8 du Rapport d'évaluation du T-CY)

- Dispositions permettant une coopération transfrontière directe avec les fournisseurs de services, par exemple :

  - Divulgation de données personnelles par une autorité de justice pénale à un fournisseur de service ou autre entité dans une juridiction étrangère, dans des circonstances spécifiques et selon des conditions spécifiques
  - Base juridique et conditions en matière de divulgation par des fournisseurs de service à des autorités de justice pénale dans des juridictions étrangères d'informations sur l'abonné
  - Requêtes directes de conservation pour les fournisseurs
  - Mesures en droit interne des pays pour l'admissibilité des données reçues de fournisseurs de services dans des juridictions étrangères en tant que preuves dans des procédures nationales
  - Procédures d'urgence pour une coopération directe avec des fournisseurs dans une juridiction étrangères, lors que la situation spécifique l'exige.

- Un cadre plus clair et des sauvegardes plus fortes pour les pratiques existantes en matière d'accès transfrontière aux données, par exemple[7]:

  - Accès transfrontière aux données par des pouvoirs obtenus dans le cadre légal

[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6

- Accès transfrontalier de bonne foi ou dans des circonstances qui l'exigent
- Le pouvoir d'administration en tant que critère de rattachement juridique

- Protection des données

  - Conditions applicables aux transferts transfrontière de données d'une autorité de justice pénale à une entité du secteur privé dans une autre juridiction
  - Conditions applicables aux transferts transfrontière de données d'une entité du secteur privé à une autorité de justice pénale dans une autre juridiction

Note :

Ces problématiques et options sont actuellement à l'examen et ne constituent pas le résultat final des travaux du Groupe Preuves dans le Cloud. Le Groupe poursuivra ses travaux en 2016, notamment par d'autres rencontres avec des fournisseurs de services et organisations de protection des données, ainsi qu'au cours des discussions en plénière du Comité de la Convention sur la cybercriminalité (T-CY), avant de soumettre ses conclusions au T-CY pour examen.

Les observations peuvent être adressées à :

Alexander Seger, Secrétaire exécutif du Comité de la Convention sur la cybercriminalité, Conseil de l'Europe, alexander.seger@coe.int