Conseil de
l'Union européenne

Bruxelles, le 28 mai 2018
(OR. en)

9418/18

Dossiers interinstitutionnels:
2018/0107 (COD)
2018/0108 (COD)

JAI 516
COPEN 166
CYBER 117
DROIPEN 76
JAIEX 56
ENFOPOL 284
DAPIX 158
EJUSTICE 62
MI 399
CODEC 873

NOTE

Origine:	la présidence
Destinataire:	Conseil
Objet:	Preuves électroniques a) règlement relatif relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale b) directive concernant les représentants légaux aux fins de la collecte de preuves en matière pénale - Débat d'orientation

I. Introduction

1. Le 17 avril 2018, la Commission a adopté deux propositions législatives: une *proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale*[1] et une *proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale*[2]. L'objet de ces propositions est d'améliorer l'accès transfrontière aux preuves numériques en créant un cadre juridique pour les décisions judiciaires adressées directement aux représentants légaux des fournisseurs de services sans intervention d'une autorité de l'État membre dans lequel est établi le représentant légal de ces fournisseurs.

[1] Doc. 8110/18.
[2] Doc. 8115/18.

Les premières discussions au niveau des experts et un débat au sein du CATS ont soulevé un certain nombre de questions politiquement importantes que la présidence souhaite mettre sur la table du Conseil (JAI) le 4 juin afin de dégager des orientations politiques en ce qui concerne non seulement la voie à suivre durant les futures négociations sur ces propositions, mais aussi les relations extérieures de l'UE dans ce domaine avec des partenaires clés comme les États-Unis.

II. Champ d'application des propositions législatives de la Commission

2. Tout en saluant les propositions, un certain nombre de délégations ont déploré que le champ d'application soit limité puisqu'il ne couvre ni *l'accès direct aux preuves numériques* (accès direct aux données sans l'assistance d'un tiers (le fournisseur de services) intermédiaire), ni *l'interception de données en temps réel*. De nombreuses délégations ont estimé que ces deux éléments devaient être pris en considération dans la mesure où ils répondent à un besoin opérationnel et doivent par conséquent être examinés plus avant et de manière beaucoup plus approfondie. Cependant, les opinions divergent quant à savoir si cet examen doit avoir lieu en vue d'inclure ces éléments dans les propositions actuelles ou, plutôt, parallèlement à celles-ci afin de ne pas retarder ou prolonger les négociations en cours.

3. En ce qui concerne *l'interception de données en temps réel*, les observations suivantes ont été formulées jusqu'ici:

   – il s'agit d'une mesure sensible et intrusive,

   – cette possibilité est prévue par la plupart des législations nationales, au niveau interne, par la directive concernant la décision d'enquête européenne et par le *CLOUD Act* des États-Unis; toute base de l'UE pour l'interception de données en temps réel devrait être envisagée dans ce cadre plus large et tenir compte de la nécessité d'équiper les autorités des États membres de la panoplie complète des outils pour lutter contre la criminalité à l'ère numérique (qui sont à la disposition de leurs collègues américains). Les États membres ont, en outre, fait valoir que la possibilité d'englober l'interception en temps réel dans un accord exécutif conclu, sur une base réciproque, en vertu du *CLOUD Act* américain, devait également être envisagée dans le cadre de la réflexion menée sur cette mesure.

4. En ce qui concerne *l'accès direct aux preuves numériques*, les observations suivantes ont été formulées jusqu'ici:

   – il s'agit d'un outil puissant en cas de perte de localisation ou lorsqu'on a à faire à des fournisseurs de services non coopératifs, permettant aux autorités des États membres d'accéder à distance aux données disponibles à la suite de la perquisition et de la saisie d'un appareil ou par le recours à des pouvoirs légalement obtenus pour accéder à un compte;

   – les législations nationales qui régissent actuellement cet accès direct varient considérablement selon les États membres, en particulier en ce qui concerne les garanties et les pouvoirs qu'elles prévoient;

   – l'éventuelle création d'un cadre commun de l'UE serait bénéfique, mais une telle approche au niveau de l'UE devrait être examinée avec prudence compte tenu de ces cadres juridiques nationaux divergents et un certain nombre de questions de droit, y compris la base juridique appropriée, devraient être soigneusement examinées.

5. ***Les ministres sont invités à procéder à un échange de vues sur l'urgence que revêt la question et sur les modalités de la poursuite des discussions sur la création d'un cadre de l'UE qui régisse "l'accès direct aux preuves numériques" et "l'interception de données en temps réel" dans un avenir proche.***

III. Évolution récente de la situation internationale et incidence du *CLOUD Act* américain

6. Le *CLOUD Act* américain[3], adopté par le Congrès des États-Unis le 23 mars 2018, précise, par un amendement au *Stored Communications Act* de 1986, que les fournisseurs de services américains sont tenus de se conformer aux injonctions américaines de divulgation de données de contenu, quel que soit l'endroit où ces données sont stockées[4]. En outre, le CLOUD Act américain permet la conclusion, à certaines conditions, d'accords exécutifs avec des gouvernement étrangers, sur la base desquels les fournisseurs de services américains pourraient communiquer directement des données de contenu aux gouvernements étrangers concernés (et intercepter des communications filaires), selon des conditions à déterminer dans les accords exécutifs.

---

[3] Clarifying Lawful Overseas Use of Data

[4] Ce qui a rendu sans objet l'affaire États-Unis contre Microsoft Corporation à ce sujet, qui soulevait la question de savoir si les autorités répressives américaines pouvaient, sur la base d'un mandat judiciaire, exiger d'un fournisseur de services installé aux États-Unis qu'il fournisse le contenu d'un compte de messagerie électronique stocké sur un serveur situé à l'étranger.

7. Lorsqu'ils ont examiné cette question lors du Conseil "JAI" de mars, les ministres se sont prononcés en faveur de l'adoption d'une approche commune de l'UE vis-à-vis des États-Unis, soulignant que cela contribuerait grandement à l'établissement de la clarté juridique pour les fournisseurs de services et pour les autorités compétentes des États membres, mais que cela éviterait également la prolifération de régimes divergents, une fragmentation au niveau de l'UE et une inégalité de traitement entre les États membres.

8. Lors de la réunion du CATS du 18 mai, la Commission et le Service juridique du Conseil ont précisé que l'UE était compétente pour entamer de telles négociations avec les États-Unis et que les États membres ne devraient pas ouvrir de négociations bilatérales. La Commission a également souligné certains des avantages exposés plus haut. Lors de la réunion ministérielle UE-États-Unis des 22 et 23 mai à Sofia, la Commission et la présidence ont également précisé la compétence de l'UE pour cette question.

9. La conclusion d'un accord exécutif entre l'UE et les États-Unis devrait également être envisagée à la lumière des dispositions de l'article 48 du RGPD, qui vient tout juste d'entrer en vigueur. Ledit article stipule que "*toute décision [...] exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international [...] entre le pays tiers demandeur et l'Union [...], sans préjudice d'autres motifs de transfert en vertu du chapitre [V]"*.

10. Enfin, lorsqu'il s'agira de définir la relation future, il conviendra d'être particulièrement attentif aux règles figurant dans les textes législatifs respectifs en ce qui concerne les cas où les fournisseurs de services sont confrontés à des législations nationales contradictoires. Le *CLOUD Act* américain contient une "clause de courtoisie"[5], alors que le projet de règlement de l'UE prévoit, à son article 15[6], une procédure de réexamen en cas d'obligations contradictoires. Il conviendra d'examiner ces dispositions de manière attentive et approfondie pour assurer la réciprocité et l'efficacité opérationnelle.

---

[5] La clause de courtoisie permet aux fournisseurs de services de demander à une juridiction américaine d'annuler ou de modifier une injonction délivrée au sujet de la conservation ou la divulgation de données si les données concernent un ressortissant non américain et si, en se conformant à l'injonction, les fournisseurs seraient amenés à violer la législation d'un pays avec lequel les États-Unis ont conclu un accord exécutif qui offre des possibilités similaires aux fournisseurs de services en vertu de la législation dont ils relèvent.

[6] L'article 15 prévoit un dialogue avec l'autorité centrale du pays tiers concerné. L'injonction européenne de production ne serait maintenue et les données ne seraient communiquées que si cette autorité ne s'y oppose pas.

11. ***Les ministres sont invités à confirmer leur souhait d'ouvrir rapidement des négociations avec les États-Unis sur la conclusion d'un accord exécutif entre l'UE et les États-Unis et sont également invités à demander à la Commission de soumettre d'urgence au Conseil une recommandation en vue d'un mandat de négociation à cet effet. Les ministres sont invités à demander à la Commission d'effectuer des démarches analogues en ce qui concerne le deuxième protocole additionnel à la convention de Budapest, actuellement en cours d'élaboration sous la houlette du Conseil de l'Europe.***