Conseil de
l'Union européenne

**Bruxelles, le 9 juin 2016**
**(OR. en)**

**10007/16**

**JAI 552**
**COPEN 195**
**DROIPEN 109**
**CYBER 67**
**JAIEX 61**
**EJUSTICE 121**

**RÉSULTATS DES TRAVAUX**

| | |
|---|---|
| Origine: | Secrétariat général du Conseil |
| en date du: | 9 juin 2016 |
| Destinataire: | délégations |
| Nº doc. préc.: | 9579/16 + COR 1 |
| Objet: | Conclusions du Conseil de l'Union européenne sur l'amélioration de la justice pénale dans le cyberespace<br>- Conclusions du Conseil (9 juin 2016) |

Les délégations trouveront en annexe les conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace, que le Conseil a adoptées lors de sa 3473e session, tenue le 9 juin 2016.

**ANNEXE**

**Conclusions du Conseil de l'Union européenne**
**sur l'amélioration de la justice pénale dans le cyberespace**

DÉTERMINÉ à empêcher les délinquants de trouver refuge dans le cyberespace,

NOTANT que les répercussions de la cybercriminalité, de la criminalité facilitée par les technologies de l'information et de la communication (TIC) ou des autres activités criminelles laissant une empreinte numérique dans le cyberespace vont grandissant,

SOULIGNANT l'importance croissante que prennent les preuves numériques dans les procédures pénales se rapportant à toutes les formes de criminalité, et en particulier le terrorisme,

SOULIGNANT l'importance, dans l'intérêt de nos économies et de nos sociétés, de protéger le cyberespace contre les utilisations à mauvais escient et les activités criminelles et, partant, de mettre à la disposition des services répressifs et des autorités judiciaires des outils efficaces pour enquêter sur les actes délictueux commis en rapport avec le cyberespace et en poursuivre les auteurs,

RAPPELANT que la lutte contre la cybercriminalité figure parmi les priorités du programme européen en matière de sécurité du 28 avril 2015, dans lequel la Commission prévoit de faire le point sur les obstacles aux enquêtes pénales sur la cybercriminalité, notamment sur les règles relatives à l'accès aux éléments de preuve et aux informations,

RAPPELANT les travaux qu'ont menés les ministres de la justice, lors de la session du Conseil "Justice et affaires intérieures" de décembre 2015[1], sur les défis qui devront être relevés à l'avenir pour assurer une justice pénale efficace à l'ère numérique,

RAPPELANT le soutien qu'ont marqué les ministres de la justice, lors de la réunion informelle du Conseil "Justice et affaires intérieures" du 26 janvier 2016, à l'élaboration d'éléments concrets d'une approche européenne commune sur les règles de compétence dans le cyberespace,

[1] Document 14369/15.

RAPPELANT la déclaration commune des ministres de la justice et des affaires intérieures et des représentants des institutions de l'UE sur les attentats terroristes perpétrés à Bruxelles, dans laquelle ils soulignent qu'il faut trouver, en priorité, des moyens de recueillir et d'obtenir plus rapidement et efficacement des preuves numériques, en intensifiant la coopération avec les pays tiers et les fournisseurs de services qui sont actifs sur le territoire européen, et permettre ainsi un meilleur respect de la législation de l'UE et des États membres et des contacts directs avec les services répressifs et, lors de la session du Conseil "Justice et affaires intérieures" de juin[2], définir des mesures concrètes pour s'attaquer à cette question complexe;

RAPPELANT la communication du 20 avril 2016 au Parlement européen, au Conseil européen et au Conseil sur la mise en œuvre du programme européen en matière de sécurité pour lutter contre le terrorisme et ouvrir la voie à une union de la sécurité réelle et effective, dans laquelle la Commission indique entendre proposer des solutions pour lever les obstacles à l'obtention de preuves numériques dans le cadre des enquêtes judiciaires.

NOTANT le rapport[3] de la conférence sur les règles de compétence dans le cyberespace tenue à Amsterdam les 7 et 8 mars 2016, qui rend compte des discussions sur les solutions éventuelles permettant d'améliorer les enquêtes dans le cyberespace, notamment en ce qui concerne les procédures d'entraide judiciaire, la coopération avec le secteur privé, et les enquêtes dans le cyberespace dans lesquelles la localisation des données ou l'origine des cyberattaques ne sont pas (encore) connues,

NOTANT que le COSI a adopté un ensemble de recommandations visant à améliorer la coopération opérationnelle dans le cadre des enquêtes pénales dans le cyberespace[4],

PRENANT NOTE de la septième série d'évaluations mutuelles actuellement en cours, qui est consacrée à la mise en œuvre pratique et au fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci,

---

[2] Document 7371/16.
[3] Document 7323/16.
[4] Document 8634/2/16 REV 2.

NOTANT les résultats du réexamen de l'accord d'entraide judiciaire entre l'UE et les États-Unis[5],

NOTANT les conclusions du Conseil sur le réseau judiciaire européen en matière de cybercriminalité[6],

RAPPELANT la convention du Conseil de l'Europe sur la cybercriminalité, du 23 novembre 2001, et son protocole additionnel, dont l'Union encourage l'utilisation en tant que cadre de référence mondial en matière de lutte contre la cybercriminalité,

RAPPELANT la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale, qui vise à rendre les enquêtes transfrontières dans l'UE plus rapides et efficaces, grâce notamment à la reconnaissance mutuelle, ainsi que la directive 2013/40/UE relative aux attaques contre les systèmes d'information, qui demande aux États membres, entre autres, de veiller à disposer d'un point de contact national opérationnel et à recourir au réseau existant de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept,

RECONNAISSANT que si ces instruments offrent des possibilités élargies aux services répressifs dans le cyberespace, des obstacles pratiques et juridiques n'en subsistent pas moins, notamment en raison de l'évolution rapide des technologies, par exemple dans les cas où l'origine de les cyberattaques ou la localisation des preuves numériques ne sont pas (encore) connues ou revêtent un caractère changeant, ou dans les cas où des réglementations contradictoires entravent la coopération avec les fournisseurs de services,

NOTANT que la cybercriminalité et la criminalité facilitée par les TIC portent atteinte aux libertés et aux droits fondamentaux et qu'il y a lieu de protéger pleinement ces droits et libertés,

RECONNAISSANT que les mesures d'enquête décidées doivent obéir à la volonté de protéger les libertés et les droits fondamentaux et être régies par les principes de nécessité et de proportionnalité,

NOTANT l'adoption de nouveaux instruments de l'UE issus de la réforme de la protection des données, et notamment la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données,

---

5 Document 9291/16.

6 Document 10025/16.

NOTANT les rapports 2012 et 2013 du groupe sur l'accès transfrontalier du comité de la convention sur la cybercriminalité, dont il ressort que plusieurs pays ont déjà poussé l'accès transfrontalier aux données plus loin, au-delà de ce que prévoit la convention de Budapest, sans base juridique claire,

RECONNAISSANT qu'il est dans l'intérêt légitime des États membres de déterminer, dans le cadre des enquêtes pénales, au minimum la localisation des preuves numériques et l'origine d'une cyberattaque,

DÉTERMINÉ à agir pour faire respecter l'État de droit dans le cyberespace,

**LE CONSEIL DE L'UNION EUROPÉENNE**

ESTIME que les lignes directrices ci-après devraient baliser les futurs travaux visant à faire mieux respecter l'État de droit dans le cyberespace et à faciliter l'obtention de preuves numériques dans le cadre des procédures pénales:

- il convient que les solutions concrètes destinées à améliorer l'efficacité des procédures pénales dans le cyberespace respectent pleinement les cadres de protection des données et des droits fondamentaux;
- il convient d'étudier la possibilité de renforcer la coopération avec les fournisseurs de services ou de mettre en place toute autre solution comparable permettant de divulguer rapidement des données; il pourrait être envisagé d'assouplir les procédures juridiques pour l'obtention de certaines catégories spécifiques de données, par exemple les données relatives aux abonnés, solution qui pourrait bénéficier à l'ensemble des parties concernées;
- il convient de rationaliser et d'accélérer les procédures d'entraide judiciaire relatives aux données électroniques; il serait possible de réduire le nombre des demandes d'entraide judiciaire entre autorités compétentes en améliorant la coopération avec les fournisseurs de services, ou par tout autre moyen comparable;

- il convient d'utiliser judicieusement les procédures de reconnaissance mutuelle afin de recueillir et d'obtenir efficacement les preuves numériques;
- il convient d'envisager d'autres mesures en se fondant sur l'examen des critère de rattachement aux fins de la détermination de la compétence d'exécution dans le cyberespace[7], y compris dans les cas où la localisation des données n'est pas (encore) connue ou revêt un caractère changeant;

JUGE nécessaire de coopérer avec les pays tiers et les acteurs privés concernés afin de conjuguer les effets des différentes mesures de manière à permettre aux services répressifs d'agir efficacement dans le cyberespace;

CONSIDÈRE qu'il faut s'atteler à titre prioritaire à définir une approche commune de l'UE destinée à améliorer la justice pénale dans le cyberespace. Les travaux menés à cet égard devraient être cohérents avec ceux en cours dans le cadre de la convention de Budapest du Conseil de l'Europe;

**en CONCLUT, PAR CONSÉQUENT, ce qui suit:**

## I. LA COOPÉRATION AVEC LES FOURNISSEURS DE SERVICES DOIT ÊTRE RENFORCÉE.

**À cette fin,**

1. Il est demandé à la COMMISSION d'élaborer un cadre commun de coopération avec les fournisseurs de services aux fins de l'obtention de certaines catégories spécifiques de données, en particulier les données concernant les abonnés, lorsque la législation des pays tiers le permet, ou toute autre solution comparable permettant la divulgation rapide et légale des données considérées[8]. La Commission est invitée à mener ces travaux en association avec les États membres et les pays tiers concernés et en coopération avec le secteur privé.

---

7 Aux fins des présentes conclusions, on entend par "compétence d'exécution" la faculté des autorités compétentes de décider d'une mesure d'enquête. En vertu des présentes conclusions, une approche commune de l'UE destinée à améliorer les enquêtes dans le cyberespace doit être étudiée, de manière à couvrir des situations spécifiques dans lesquelles les cadres existants sont insuffisants.

8 Lorsque la demande de données suppose le transfert, par l'autorité compétente d'un État membre, de données à caractère personnel, la législation applicable en matière de protection des données doit être respectée.

2. Les solutions retenues devraient énoncer les exigences arrêtées d'un commun accord, y compris les exigences de nécessité et de proportionnalité applicables aux demandes adressées aux fournisseurs de services en vue d'un accès légal aux données qu'ils détiennent. Les solutions considérées devrait tendre à empêcher les interprétations incohérentes et les conflits entre les réglementations existantes et à régler la question de la non-divulgation des demandes de données. Les solutions proposées ne doivent pas entraver les dispositions prises au niveau national.

3. À cet effet, il est demandé à la COMMISSION, en association avec les États membres, d'étudier avec les fournisseurs de services la possibilité d'utiliser des formulaires et des outils normalisés tel que ceux visés à la section II, afin de faciliter l'authentification, de mettre en place des procédures rapides et de renforcer la transparence du processus de recueil et d'obtention de preuves numériques ainsi que l'obligation de rendre des comptes dans ce cadre.

   *Il est demandé à la Commission de présenter au plus tard en décembre 2016 un rapport sur l'état d'avancement des travaux sur ce dossier et au plus tard en juin 2017 les résultats escomptés.*

## II. LES PROCÉDURES D'ENTRAIDE JUDICIAIRE (ET, LE CAS ÉCHÉANT, DE RECONNAISSANCE MUTUELLE) DOIVENT ÊTRE RATIONALISÉES.

**À cette fin,**

4. Il est demandé à la COMMISSION d'étudier à titre prioritaire, en association avec les ÉTATS MEMBRES et, lorsqu'il y a lieu, avec les pays tiers, les moyens permettant de recueillir et d'obtenir plus rapidement et efficacement des preuves numériques, en rationalisant l'utilisation des procédures d'entraide judiciaire et, le cas échéant, de reconnaissance mutuelle.
5. À cet effet, il est demandé à la COMMISSION d'examiner et de formuler, en association avec les ÉTATS MEMBRES, EUROJUST et les pays tiers, des recommandations quant à la manière d'adapter, lorsqu'il y a lieu, les procédures et les formulaires normalisés existants aux fins du recueil et de l'obtention de preuves numériques.
6. Pour rendre plus efficace l'utilisation des procédures et des formulaires normalisés aux fins de l'obtention de preuves numériques, il est demandé à la COMMISSION de mettre au point, en association avec les ÉTATS MEMBRES, EUROJUST, le CEPOL et, lorsqu'il y a lieu, les pays tiers, au moyen, le cas échéant, des outils électroniques existants et dans le respect des compétences et des canaux de communication prévus par les cadres juridiques actuels:
    - un portail en ligne sécurisé pour les demandes et les réponses électroniques relatives aux preuves numériques et les procédures correspondantes, y compris pour ce qui est de l'utilisation facultative de traductions automatisées des demandes, ainsi du suivi et de la traçabilité des demandes;
    - en coopération avec le Réseau européen de formation judiciaire, le réseau judiciaire européen en matière de cybercriminalité et, lorsqu'il y a lieu, les autorités des pays tiers, des lignes directrices et des modules de formation spécifiques concernant l'utilisation efficace des cadres existants utilisés aux fins du recueil et de l'obtention de preuves numériques, y compris des lignes directrices précisant les situations dans lesquelles les règles existantes prévoient que le recours à l'entraide judiciaire ou aux instruments de reconnaissance mutuelle n'est pas requis.

*Il est demandé à la COMMISSION de présenter au plus tard en décembre 2016 un rapport à mi-parcours sur l'état d'avancement de ces activités et au plus tard en juin 2017 les résultats escomptés. Il est demandé à la COMMISSION de présenter le portail en ligne au plus tard en décembre 2017.*

7. Il est demandé à la COMMISSION, en association avec les ÉTATS MEMBRES et, lorsqu'il y a lieu, les pays tiers, d'étudier des mesures supplémentaires permettant de rendre plus efficaces le recueil et l'obtention de preuves numériques, notamment grâce à l'utilisation du cadre d'entraide judiciaire UE-États-Unis.
8. Il est demandé à la COMMISSION, dans l'optique d'une utilisation pleine et entière de la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale, de continuer de suivre et de soutenir les États membres dans le cadre du processus de transposition de cette directive, qui doit être achevé le 22 mai 2017.
9. Il est demandé aux ÉTATS MEMBRES de:
   - ratifier et appliquer intégralement la convention sur la cybercriminalité du 23 novembre 2001;
   - transposer rapidement la directive concernant la décision d'enquête européenne en matière pénale, pour le 22 mai 2017 au plus tard;
   - veiller à disposer des capacités nécessaires pour traiter les demandes d'entraide judiciaire relatives à des enquêtes dans le cyberespace et fournir aux agents concernés la formation requise quant à la manière de traiter ces demandes;
   - optimiser l'utilisation des points de contact existants disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept et recourir plus fréquemment aux équipes communes d'enquête afin de faciliter l'échange d'informations et/ou d'accélérer les procédures d'entraide judiciaire.

## III. IL CONVIENT DE RÉEXAMINER LES RÈGLES RELATIVES À LA COMPÉTENCE D'EXÉCUTION DANS LE CYBERESPACE.

**À cette fin,**

10. LA COMMISSION est invitée, à la lumière des orientations politiques que fourniront les ministres de la justice lors de la session du Conseil de juin 2016 et en association avec les ÉTATS MEMBRES, EUROJUST et EUROPOL, à étudier les possibilités de définir une approche commune de l'UE concernant la compétence d'exécution dans le cyberespace dans des situations dans lesquelles les cadres existants ne sont pas suffisants, par exemple lorsque différents systèmes d'information sont utilisés simultanément dans plusieurs juridictions pour commettre un seul délit, lorsque des preuves électroniques pertinentes se déplacent d'une juridiction à l'autre dans de courts laps de temps, ou lorsque des méthodes sophistiquées sont utilisées pour dissimuler le lieu où se trouvent des preuves électroniques ou le lieu de l'activité criminelle, entraînant une "disparition du lieu"[9].

11. Tout en tenant compte des spécificités de chaque situation, l'approche en question devrait déterminer:

- quels critères de rattachement peuvent servir à établir la compétence d'exécution dans le cyberespace;
- s'il est possible de recourir à des mesures d'enquête indépendamment des frontières physiques et, dans l'affirmative, quels types de mesures.

12. Il convient de réfléchir:

- à la nature et à la gravité des délits susceptibles de rester impunis;
- aux éléments pouvant servir à établir la compétence d'exécution, c'est-à-dire sur la base de critères de rattachement tels que, par exemple, le lieu d'établissement d'un prestataire de services, l'activité économique d'un prestataire de services dans l'État menant l'enquête - lorsque le prestataire de services propose des produits ou des services sur le territoire de l'État qui mène l'enquête ("lien commercial") -, le lieu de résidence habituelle et/ou la nationalité de la personne accusée ou suspectée, et/ou le lieu où se trouve la personne concernée;

[9] Il ne s'agit que d'exemples. La Commission est invitée à réfléchir à des solutions susceptibles de répondre à de telles situations ou à des situations de gravité comparable justifiant une telle approche.

- au recours aux injonctions internes de production et à l'efficacité de telles injonctions, sur la base des critères de rattachement possibles précités, aux fins de la compétence d'exécution dans le cyberespace;
- à une solution en matière de coopération aux fins de l'accès transfrontière direct aux données sans assistance technique;
- à des garanties appropriées, notamment la protection des droits et libertés fondamentaux et des données à caractère personnel, ainsi que la proportionnalité et la subsidiarité en tant que principes directeurs pour le recours aux mesures d'enquête afin de garantir leur caractère licite;
- à d'éventuelles analogies avec d'autres régimes juridiques transfrontières, par exemple le traité sur le régime "ciel ouvert" et la convention sur le droit de la mer, la réglementation européenne en matière de protection des données et le droit de la concurrence de l'UE;
- à l'incidence d'une telle approche sur le cadre juridique existant.

*LA COMMISSION est invitée à rendre compte du processus d'élaboration de cette approche au plus tard en décembre 2016 et à présenter les résultats de cette évaluation d'ici juin 2017. L'évaluation devrait notamment porter sur des éléments spécifiques en vue d'une approche commune de l'UE et des propositions pour la réalisation de celle-ci, y compris la possibilité de mener une initiative législative à cet égard.*