COM (2019) 71 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2018-2019

Reçu à la Présidence de l'Assemblée nationale
le 8 février 2019

Enregistré à la Présidence du Sénat
le 8 février 2019

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Recommandation de décision du Conseil autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185)

E 13807

Conseil de
l'Union européenne

Bruxelles, le 5 février 2019
(OR. en)

6110/19

JAI 101
COPEN 44
CYBER 35
DROIPEN 17
JAIEX 9
ENFOPOL 46
DAPIX 42
EJUSTICE 15
MI 113
TELECOM 51
DATAPROTECT 28
USA 9
RELEX 98

NOTE DE TRANSMISSION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	5 février 2019
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2019) 71 final
Objet:	Recommandation de DÉCISION DU CONSEIL autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185)

Les délégations trouveront ci-joint le document COM(2019) 71 final.

p.j.: COM(2019) 71 final

COMMISSION
EUROPÉENNE

Bruxelles, le 5.2.2019
COM(2019) 71 final

Recommandation de

DÉCISION DU CONSEIL

autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185)

EXPOSÉ DES MOTIFS

1. CONTEXTE

L'évolution des technologies de l'information et de la communication – tout en offrant des possibilités sans précédent pour l'humanité – pose également des défis, y compris pour la justice pénale et donc pour l'état de droit dans le cyberespace. Alors que la cybercriminalité et d'autres infractions impliquant des preuves électroniques dans des systèmes informatiques sont en plein essor et alors que les preuves relatives à ces infractions sont de plus en plus souvent stockées sur des serveurs situés dans des juridictions étrangères, multiples, changeantes ou inconnues, à savoir dans le nuage, les pouvoirs des services répressifs demeurent restreints par les limites territoriales.

En avril 2015, dans le programme européen en matière de sécurité[1], la Commission européenne s'est engagée à faire le point sur les obstacles aux enquêtes pénales sur la criminalité facilitée par internet, notamment concernant l'accès transfrontière aux preuves électroniques. Le 17 avril 2018, la Commission a proposé au Conseil et au Parlement européen un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[2], ainsi qu'une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale[3] («propositions relatives aux preuves électroniques»). Ces propositions ont pour but d'accélérer dans l'Union le processus pour recueillir et obtenir des preuves électroniques qui sont stockées et/ou détenues par des fournisseurs de services établis dans une autre juridiction.

La convention sur la cybercriminalité du Conseil de l'Europe

La convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185) a pour objectif de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques. Elle 1) contient des dispositions harmonisant les éléments constitutifs des infractions en droit pénal matériel national et des dispositions connexes dans le domaine de la cybercriminalité, elle 2) prévoit les pouvoirs nécessaires en droit pénal procédural national pour les enquêtes et les poursuites concernant ces infractions ainsi que d'autres infractions commises au moyen d'un système informatique ou dont les preuves sont sous forme électronique, et elle 3) vise à mettre en place un système rapide et efficace de coopération internationale. La convention est ouverte aux États membres du Conseil de l'Europe et aux pays tiers. 62 pays sont actuellement parties à la convention, y compris 26 États membres de l'Union européenne[4]. La convention ne prévoit pas que l'Union européenne puisse adhérer à la convention. L'Union européenne est néanmoins reconnue comme une organisation observateur au comité de la convention sur la cybercriminalité (T-CY). À ce titre, elle prend part aux réunions du comité de la convention.

---

1 Communication de la Commission au Parlement européen et au Conseil: Le programme européen en matière de sécurité, 28 avril 2015, COM(2015) 185 final.

2 Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 17 avril 2018, COM(2018) 225 final.

3 Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, 17 avril 2018, COM(2018) 226 final.

4 Tous sauf l'Irlande et la Suède, qui ont signé mais pas ratifié la convention, tout en s'étant engagées à y adhérer.

L'article 46, paragraphe 1, point c), de la convention dispose que les parties se concertent périodiquement, au besoin, afin de faciliter l'examen de l'éventualité de compléter ou d'amender la convention. Les parties à la convention sur la cybercriminalité examinent depuis un certain temps les défis qui se posent et les obstacles qui empêchent les autorités judiciaires et policières nationales d'accéder aux preuves électroniques d'infractions faisant l'objet d'une enquête pénale qui sont sous forme de données informatiques, à savoir de 2012 à 2014, dans le cadre d'un groupe de travail sur l'accès transfrontalier aux données, et de 2015 à 2017, dans le cadre du groupe sur les preuves dans le nuage.

Négociations en vue d'un deuxième protocole additionnel à la convention

À la suite des propositions du groupe sur les preuves dans le nuage[5], le comité de la convention sur la cybercriminalité (T-CY) a adopté plusieurs recommandations, y compris concernant la négociation d'un deuxième protocole additionnel à la convention sur la cybercriminalité[6] relatif à la coopération internationale renforcée (ci-après le «deuxième protocole additionnel»). En juin 2017, le comité de la convention sur la cybercriminalité a approuvé le mandat pour la préparation d'un deuxième protocole additionnel à la convention au cours de la période de septembre 2017 à décembre 2019.

Conformément au mandat, le deuxième protocole additionnel peut contenir les éléments suivants:

- dispositions pour une entraide juridique plus efficace, notamment:
  - un régime simplifié pour les demandes d'entraide juridique concernant des informations sur les abonnés;
  - des injonctions de produire internationales;
  - une coopération directe entre autorités judiciaires pour les demandes d'entraide;
  - des enquêtes et équipes d'enquête communes;
  - des demandes formulées en anglais;
  - l'audition audio/vidéo des témoins, des victimes et des experts;
  - des procédures d'urgence pour les demandes d'entraide;
- dispositions permettant la coopération directe avec des fournisseurs de services dans d'autres juridictions pour ce qui est des demandes relatives à des informations sur les abonnés, des demandes de conservation et des demandes en urgence;
- un cadre plus clair et des garanties plus fortes concernant les pratiques existantes en matière d'accès transfrontière aux données;
- des garanties, notamment des conditions relatives à la protection des données.

Les négociations des différentes dispositions du deuxième protocole additionnel progressent à des rythmes différents. La situation actuelle dans les groupes de travail sur les quatre axes de travail principaux énoncés dans le mandat est la suivante:

---

5 Rapport final du groupe sur les preuves dans le nuage du T-CY intitulé «Accès de la justice pénale aux preuves électroniques dans le cloud: Recommandations pour examen par le T-CY», du 16 septembre 2016.

6 Le premier protocole additionnel (STE n° 189) à la convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques était ouvert à la signature des États signataires de la convention en 2003. 31 pays sont parties au premier protocole additionnel, notamment 17 États membres de l'UE.

- les dispositions sur «la langue dans laquelle doit être formulée une demande» et «les procédures d'urgence pour les demandes d'entraide» ont fait l'objet d'une adoption préliminaire par la plénière de rédaction du protocole en juillet 2018;
- les dispositions sur la «vidéoconférence» ont fait l'objet d'une adoption préliminaire par la plénière de rédaction du protocole en novembre 2018;
- la plénière de rédaction du protocole qui s'est tenue en novembre 2018 a également permis de mener des discussions approfondies (dispositions sur «la juridiction» et «le modèle d'approbation») et de procéder à des mises à jour («la coopération directe avec les fournisseurs de services», «les injonctions de produire internationales», «l'extension des recherches/accès sur la base des pouvoirs», «enquêtes conjointes et équipes conjointes d'enquête» et «techniques d'enquête»);
- les progrès n'ont pas été suffisants dans d'autres domaines (garanties, notamment des conditions relatives à la protection des données).

2. OBJECTIFS DE LA PROPOSITION

La présente recommandation est soumise au Conseil afin que celui-ci autorise la participation aux négociations au nom de l'Union européenne et de ses États membres sur un deuxième protocole additionnel, qu'il adopte des directives de négociation et qu'il désigne la Commission en tant que négociateur conformément au projet de directives en annexe, en vertu de l'article 218 du TFUE.

L'article 3, paragraphe 2, du TFUE prévoit que l'Union dispose d'une compétence exclusive «*pour la conclusion d'un accord international [...] dans la mesure où elle est susceptible d'affecter des règles communes ou d'en altérer la portée*». Un accord international peut affecter des règles communes ou en altérer la portée lorsque le domaine qu'il régit recouvre la législation de l'Union ou est déjà couvert en grande partie par le droit de l'Union.

L'Union européenne a adopté des règles communes sur la base de l'article 82, paragraphe 1, et de l'article 16 du TFUE sur des éléments examinés en vue du deuxième protocole additionnel. Le cadre juridique actuel de l'Union contient notamment des instruments concernant une coopération des services répressifs et judiciaires en matière pénale, comme la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale[7], la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[8], le règlement (UE) 2018/1727 relatif à Eurojust[9], le règlement (UE) 2016/794 relatif à Europol[10], la décision-cadre 2002/465/JAI du Conseil relative aux équipes communes d'enquête[11], et la décision-cadre 2009/948/JAI du Conseil relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des

[7] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

[8] Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (JO C 197 du 12.7.2000, p. 1).

[9] Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI (JO L 295 du 21.11.2018, p. 138).

[10] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

[11] Décision-cadre 2002/465/JAI du Conseil du 13 juin 2002 relative aux équipes communes d'enquête (JO L 162 du 20.6.2002, p. 1).

procédures pénales[12]. En outre, l'Union a adopté plusieurs directives qui renforcent les droits procéduraux des suspects et des personnes poursuivies[13].

Sur le plan extérieur, l'Union a conclu un certain nombre d'accords bilatéraux avec des pays tiers, comme les accords d'entraide judiciaire en matière pénale entre l'Union et les États-Unis d'Amérique[14] et entre l'Union et le Japon[15].

La protection des données à caractère personnel est un droit fondamental inscrit dans les traités de l'UE et dans la charte des droits fondamentaux de l'UE et les données à caractère personnel peuvent uniquement faire l'objet d'un traitement conformément au règlement (UE) 2016/679 (le «règlement général sur la protection des données»)[16] et la directive (UE) 2016/680 (la «directive sur la protection des données policières»)[17]. La charte des droits fondamentaux consacre également le droit fondamental de toute personne au respect de sa vie privée et familiale, de son domicile, ainsi que de ses communications, et le respect de la confidentialité de ses communications constitue un élément essentiel de ce droit. Les données de communications électroniques peuvent uniquement être traitées conformément à la directive 2002/58/CE (la «directive vie privée et communications électroniques»)[18].

---

12 Décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales (JO L 328 du 15.12.2009, p. 42).

13 Directive 2010/64/UE du Parlement européen et du Conseil du 20 octobre 2010 relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales (JO L 280 du 26.10.2010, p. 1); directive 2012/13/UE du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales (JO L 142 du 1.6.2012, p. 1); directive 2013/48/UE du Parlement européen et du Conseil du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires (JO L 294 du 6.11.2013, p. 1); directive (UE) 2016/1919 du Parlement européen et du Conseil du 26 octobre 2016 concernant l'aide juridictionnelle pour les suspects et les personnes poursuivies dans le cadre des procédures pénales et pour les personnes dont la remise est demandée dans le cadre des procédures relatives au mandat d'arrêt européen (JO L 297 du 4.11.2016, p. 1); directive (UE) 2016/800 du Parlement européen et du Conseil du 11 mai 2016 relative à la mise en place de garanties procédurales en faveur des enfants qui sont des suspects ou des personnes poursuivies dans le cadre des procédures pénales (JO L 132 du 21.5.2016, p. 1); directive (UE) 2016/343 du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales (JO L 65 du 11.3.2016, p. 1); directive 2012/13/UE du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales.

14 Décision 2009/820/PESC du Conseil du 23 octobre 2009 concernant la conclusion, au nom de l'Union européenne, de l'accord d'extradition entre l'Union européenne et les États-Unis d'Amérique et de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique (JO L 291 du 7.11.2009, p. 40).

15 Accord entre l'Union européenne et le Japon relatif à l'entraide judiciaire en matière pénale (JO L 39 du 12.2.2010, p. 20).

16 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (JO L 119 du 4.5.2016, p. 1).

17 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

18 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37), modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009

En outre, pour déterminer si un domaine est déjà couvert en grande partie par des règles communes, il convient de prendre en compte non seulement l'état actuel du droit de l'Union dans le domaine concerné, mais également ses perspectives d'évolution, dans la mesure où celles-ci sont prévisibles au moment de cette analyse. Le domaine couvert par le deuxième protocole additionnel est directement lié aux perspectives d'évolution prévisibles des règles communes pertinentes. À cet égard, les propositions de la Commission d'avril 2018 sur l'accès transfrontière aux preuves électroniques sont également pertinentes[19].

Le champ d'application des propositions couvre des types spécifiques de fournisseurs de services opérant dans l'Union européenne. Un fournisseur propose des services dans l'Union européenne lorsqu'il permet aux utilisateurs d'un ou de plusieurs États membres d'utiliser ses services et lorsqu'il a un lien substantiel avec l'Union, par exemple lorsqu'il possède un établissement dans un État membre ou lorsqu'il fournit des services à un grand nombre d'utilisateurs dans cet État membre. Les fournisseurs qui ne sont pas présents dans l'Union sont obligés de désigner un représentant légal à qui il est possible d'adresser des injonctions de production.

Dans ses conclusions du 18 octobre 2018, le Conseil européen déclarait qu'«*[i]l y a lieu de trouver des solutions pour assurer un accès transfrontière rapide et effectif aux preuves numériques afin de lutter efficacement contre le terrorisme et d'autres formes de grande criminalité organisée, tant au sein de l'UE qu'au niveau international; il convient, d'ici la fin de la législature, de parvenir à un accord concernant les propositions de la Commission sur les preuves électroniques et l'accès aux informations financières, ainsi que sur l'amélioration de la lutte contre le blanchiment de capitaux. Par ailleurs, la Commission devrait présenter d'urgence des mandats de négociation pour les négociations internationales sur les preuves électroniques*».

Les propositions de la Commission relatives aux preuves électroniques permettent une approche coordonnée et cohérente tant au sein de l'Union européenne que par celle-ci au niveau international, dans le respect des règles de l'Union, notamment en matière de non-discrimination entre les États membres de l'Union et entre leurs ressortissants. Tandis que, dans son analyse d'impact des propositions relatives aux preuves électroniques, la Commission constatait déjà que les propositions pouvaient être utilement complétées par des accords bilatéraux ou multilatéraux sur l'accès transfrontière aux preuves électroniques intégrant les garanties nécessaires, elle a décidé de proposer des règles de l'UE sur les modalités et garanties appropriées pour l'accès transfrontière aux preuves électroniques, avant de s'engager dans des négociations internationales avec des tiers[20].

Au niveau international, la Commission a continué de participer en tant qu'observateur aux discussions connexes qui se sont déroulées dans le cadre de la convention sur la

---

modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

19 Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 17 avril 2018, COM(2018) 225 final; proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, 17 avril 2018, COM(2018) 226 final.

20 Alors que les négociations avec le Parlement européen et le Conseil sont en cours, ce dernier a approuvé une orientation générale concernant la proposition de la Commission relative à un règlement lors de la session du Conseil «Justice et affaires intérieures» du 7 décembre 2018.

cybercriminalité du Conseil de l'Europe[21]. L'accès transfrontière aux preuves électroniques a été régulièrement abordé lors des dernières réunions ministérielles UE-États-Unis consacrées à la justice et aux affaires intérieures.

Les deux recommandations en vue de participer aux négociations du deuxième protocole additionnel à la convention sur la cybercriminalité et d'ouvrir des négociations avec les États-Unis d'Amérique font l'objet d'une adoption simultanée par la Commission. Tandis que les deux processus progresseront à des rythmes différents, ils portent sur des questions interdépendantes et les engagements pris dans une négociation peuvent avoir une incidence directe sur les autres volets des négociations.

Les propositions relatives aux preuves électroniques traitant de la situation de types spécifiques de fournisseurs de services opérant sur le marché de l'Union, il existe un risque que certaines obligations soient en contradiction avec la législation des pays tiers. Afin de remédier à ces conflits de lois, et conformément au principe de courtoisie internationale, les propositions relatives aux preuves électroniques contiennent des dispositions prévoyant des mécanismes spécifiques pour les cas où un prestataire de services est confronté à des obligations contradictoires découlant de la législation d'un pays tiers lorsque des preuves sont demandées. Ces mécanismes comprennent une procédure de réexamen pour clarifier la situation. Le deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe devrait avoir pour objectif d'éviter les obligations contradictoires entre les parties à cette convention.

Il peut donc être considéré que la conclusion du deuxième protocole additionnel est susceptible d'affecter des règles communes ou d'en altérer la portée.

En conséquence, l'Union dispose d'une compétence exclusive pour la négociation du deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (en vertu de l'article 3, paragraphe 2, du TFUE).

L'objet du deuxième protocole additionnel relève des politiques et compétences de l'UE, notamment dans le domaine des instruments relatifs à la coopération judiciaire en matière pénale (article 82, paragraphe 1, du TFUE) et à la protection des données (article 16 du TFUE) et, au regard du droit de l'UE, les négociations ne pourraient avoir lieu sans la participation de l'Union. De plus, la Commission est chargée, d'une manière générale, de la représentation de l'Union européenne en vertu de l'article 17, paragraphe 1, du TUE. Au vu de ce qui précède, la Commission devrait être désignée par le Conseil en tant que négociateur du deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185).

3. DISPOSITIONS PERTINENTES DANS LE DOMAINE D'ACTION

Les négociations devraient garantir que les dispositions convenues sont compatibles avec le droit de l'Union et les obligations qui incombent aux États membres en vertu de celui-ci, compte tenu également de ses perspectives d'évolution. De plus, il faudra veiller à ce que le deuxième protocole additionnel comporte une clause de déconnexion permettant aux États membres de l'Union qui deviennent parties au deuxième protocole additionnel d'établir les relations entre eux sur la base du droit de l'Union. En particulier, le fonctionnement des propositions de la Commission européenne relatives aux preuves électroniques, y compris à mesure qu'elles évoluent au cours des négociations entre les colégislateurs dans le cadre de la

[21] Convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest, STE n° 185), 23 novembre 2001, http://conventions.coe.int.

procédure législative et finalement sous leur forme définitive (adoptée), devrait être assuré entre les États membres de l'Union.

Le deuxième protocole additionnel devrait contenir les garanties nécessaires pour les libertés et droits fondamentaux reconnus par la charte des droits fondamentaux de l'Union européenne, notamment le droit au respect de la vie privée et familiale, du domicile et des communications, reconnu à l'article 7 de la charte, le droit à la protection des données à caractère personnel, reconnu à l'article 8 de la charte, le droit à un recours effectif et à accéder à un tribunal impartial, reconnu à l'article 47 de la charte, la présomption d'innocence et les droits de la défense, reconnus à l'article 48 de la charte, et les principes de légalité et de proportionnalité des délits et des peines, reconnus à l'article 49 de la charte. Il convient que le deuxième protocole additionnel soit appliqué conformément à ces droits et principes.

Des garanties appropriées en matière de protection des données et de la vie privée pour la collecte, le transfert et l'utilisation ultérieure des données à caractère personnel et des données de communications électroniques doivent être inscrites dans le protocole, de manière à assurer le plein respect par les fournisseurs de services de l'UE des obligations qui leur incombent en vertu de la législation de l'UE en matière de protection des données et de la vie privée, dans la mesure où un tel accord international pourrait servir de base juridique à des transferts de données à la suite d'injonctions ou de demandes de production émises par une autorité d'un État non membre de l'UE partie au protocole additionnel exigeant qu'un responsable du traitement ou un sous-traitant communique des données à caractère personnel et des données de communications électroniques. Ces garanties devraient donc permettre la protection des libertés et droits fondamentaux des citoyens de l'UE, notamment la protection de la vie privée et des données à caractère personnel lorsque des données à caractère personnel ou des données de communications électroniques sont communiquées à des services répressifs de pays non membres de l'Union européenne.

Compte tenu de l'absence de dispositions permettant aux autorités d'accéder aux données sans l'aide d'un intermédiaire («accès direct») dans les propositions de la Commission européenne relatives aux preuves électroniques, tout recours à ce type de mesures peut uniquement être fondé sur le droit national. S'il est possible que le deuxième protocole additionnel contienne des dispositions relatives à «l'extension des recherches et l'accès sur la base des pouvoirs» et aux «techniques d'enquête», l'objectif principal devrait être de renforcer les garanties concernant ledit accès transfrontière direct aux données afin d'assurer la protection des libertés et des droits fondamentaux des citoyens de l'Union, notamment la protection de la vie privée et des données à caractère personnel.

La conclusion du deuxième protocole additionnel devrait permettre la conclusion d'accords ou traités bilatéraux entre les parties au protocole ou entre les parties au protocole et l'Union européenne, qui régiraient leurs relations. À cette fin, il y a lieu d'insérer une clause adaptée prévoyant que, si deux ou plusieurs parties à la convention ont déjà conclu un accord ou un traité relatif aux matières traitées par la convention, ou si elles devaient le faire à l'avenir, elles ont la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, dès lors qu'elles le font d'une manière qui soit compatible avec les objectifs et principes de la convention. L'accord entre l'Union européenne et les États-Unis sur l'accès transfrontière aux preuves électroniques aux fins de la coopération judiciaire en matière pénale devrait, dans le cadre des relations entre les États-Unis d'Amérique et l'Union européenne, prévaloir sur tout accord ou arrangement trouvé lors des négociations du deuxième protocole additionnel, dans la mesure où il couvre les mêmes questions.

Recommandation de

DÉCISION DU CONSEIL

autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 218, paragraphes 3 et 4,

vu la recommandation de la Commission européenne,

considérant ce qui suit:

(1) Le 9 juin 2017, le comité de la convention sur la cybercriminalité (STE n° 185) du Conseil de l'Europe a arrêté une décision adoptant le mandat pour la préparation d'un deuxième protocole additionnel à la convention.

(2) Le mandat relatif au deuxième protocole additionnel contient les éléments de réflexion suivants: des dispositions pour une entraide juridique plus efficace (un régime simplifié pour les demandes d'entraide concernant des informations sur les abonnés; des injonctions de produire internationales; une coopération directe entre autorités judiciaires pour les demandes d'entraide; des enquêtes et équipes d'enquête communes; des demandes formulées en anglais; l'audition audio/vidéo des témoins, des victimes et des experts; des procédures d'urgence pour les demandes d'entraide); des dispositions permettant la coopération directe avec des fournisseurs de services dans d'autres juridictions pour ce qui est des demandes relatives à des informations sur les abonnés, des demandes de conservation et des demandes en urgence; un cadre plus clair et des garanties plus fortes concernant les pratiques existantes en matière d'accès transfrontière aux données; des garanties, notamment des conditions relatives à la protection des données.

(3) L'Union a adopté des règles communes qui couvrent déjà en grande partie les éléments envisagés pour le deuxième protocole additionnel, notamment un ensemble complet d'instruments visant à faciliter la coopération judiciaire en matière pénale[22] et

[22] Acte du Conseil du 29 mai 2000 établissant la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (JO C 197 du 12.7.2000, p. 1); règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO L 295 du 21.11.2018, p. 138); règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53); décision-cadre 2002/465/JAI du Conseil du 13 juin 2002 relative aux équipes communes d'enquête (JO L 162 du 20.6.2002, p. 1); décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales (JO L 328 du 15.12.2009, p. 42); directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

à garantir des normes minimales pour les droits procéduraux[23], ainsi que des garanties en matière de protection des données et de la vie privée[24].

(4) La Commission a également présenté une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, ainsi qu'une proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, qui instaurent des injonctions européennes transfrontières contraignantes de production et de conservation à adresser directement à un représentant d'un fournisseur de services dans un autre État membre[25].

(5) Dès lors, le deuxième protocole additionnel est susceptible d'affecter des règles communes de l'Union ou d'en altérer la portée.

(6) L'article 82, paragraphe 1, et l'article 16 du traité sur le fonctionnement de l'Union européenne précisent les compétences de l'Union dans les domaines de la coopération judiciaire en matière pénale, ainsi que de la protection des données et de la vie privée. Afin de préserver l'intégrité du droit de l'Union et de garantir la cohérence entre les dispositions du droit international et du droit de l'Union, il est nécessaire que l'Union participe aux négociations sur le deuxième protocole additionnel.

(7) Le deuxième protocole additionnel devrait contenir les garanties nécessaires pour les libertés et droits fondamentaux, notamment le droit à la protection des données à caractère personnel et de la vie privée, le droit au respect de la vie privée et familiale, du domicile et des communications, reconnu à l'article 7 de la charte, le droit à la protection des données à caractère personnel, reconnu à l'article 8 de la charte, le droit à un recours effectif et à accéder à un tribunal impartial, reconnu à l'article 47 de la charte, la présomption d'innocence et les droits de la défense, reconnus à l'article 48 de la charte, et les principes de légalité et de proportionnalité des délits et des peines, reconnus à l'article 49 de la charte. Le deuxième protocole additionnel devrait être appliqué conformément à ces droits et principes.

---

[23] Directive 2010/64/UE du Parlement européen et du Conseil du 20 octobre 2010 relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales (JO L 280 du 26.10.2010, p. 1); directive 2012/13/UE du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales (JO L 142 du 1.6.2012, p. 1); directive 2013/48/UE du Parlement européen et du Conseil du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires (JO L 294 du 6.11.2013, p. 1); directive (UE) 2016/1919 du Parlement européen et du Conseil du 26 octobre 2016 concernant l'aide juridictionnelle pour les suspects et les personnes poursuivies dans le cadre des procédures pénales et pour les personnes dont la remise est demandée dans le cadre des procédures relatives au mandat d'arrêt européen (JO L 297 du 4.11.2016, p. 1); directive (UE) 2016/800 du Parlement européen et du Conseil du 11 mai 2016 relative à la mise en place de garanties procédurales en faveur des enfants qui sont des suspects ou des personnes poursuivies dans le cadre des procédures pénales (JO L 132 du 21.5.2016, p. 1).

[24] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (JO L 119 du 4.5.2016, p. 1); directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

[25] COM(2018) 225 final et COM(2018) 226 final.

(8) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement et du Conseil[26] et a rendu son avis le ...[27],

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La Commission est autorisée à négocier, au nom de l'Union, le deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185).

Article 2

Les directives de négociation figurent en annexe.

Article 3

Les négociations sont conduites en concertation avec un comité spécial devant être désigné par le Conseil.

Article 4

La Commission est destinataire de la présente décision.

Fait à Bruxelles, le

Par le Conseil
Le président

[26] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[27] JO C ...