COM (2019) 70 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 l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale

E 13806

Conseil de
l'Union européenne

Bruxelles, le 5 février 2019
(OR. fr)

6102/19

JAI 100
COPEN 43
CYBER 34
DROIPEN 16
JAIEX 8
ENFOPOL 45
DAPIX 41
EJUSTICE 14
MI 111
TELECOM 50
DATAPROTECT 27
USA 8
RELEX 97

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) 70 final
Objet:	Recommandation de DÉCISION DU CONSEIL autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale

Les délégations trouveront ci-joint le document COM(2019) 70 final.

p.j.: COM(2019) 70 final

COMMISSION
EUROPÉENNE

Bruxelles, le 5.2.2019
COM(2019) 70 final

Recommandation de

DÉCISION DU CONSEIL

autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale

EXPOSÉ DES MOTIFS

1. CONTEXTE

Les flux de données transfrontières augmentent avec l'utilisation croissante des médias sociaux, du courrier web, des services de messagerie et des applications pour communiquer, travailler, nouer des contacts et obtenir des informations, y compris à des fins illicites. De plus en plus d'enquêtes pénales reposent donc sur des preuves électroniques qui ne sont pas accessibles au public. Compte tenu de la nature transfrontière de l'internet et de la possibilité de fournir des services depuis n'importe quel endroit dans le monde, y compris par des entreprises non européennes, il est urgent de faciliter l'accès transfrontière aux preuves électroniques pour pratiquement tous les types d'infraction. Les récents attentats terroristes, en particulier, ont fait apparaître la nécessité de trouver en priorité des moyens permettant aux procureurs et aux juges des États membres de l'Union européenne de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement.

Plus de la moitié de l'ensemble des enquêtes pénales exigent aujourd'hui d'accéder à des preuves électroniques transfrontières. Des preuves électroniques sont nécessaires dans près de 85 % des enquêtes pénales et, dans les deux tiers des cas, il y a lieu d'obtenir les preuves auprès de fournisseurs de services en ligne établis dans une autre juridiction. Le nombre de demandes adressées aux principaux fournisseurs de services en ligne a augmenté de 84 % entre 2013 et 2018. Ces types de données sont essentiels dans les enquêtes pénales pour pouvoir identifier une personne ou obtenir des informations sur ses activités.

Les preuves électroniques recouvrent différents types de données sous forme électronique qui sont utiles dans les enquêtes et les poursuites pénales, et sont souvent stockées sur les serveurs des fournisseurs de services en ligne. Il s'agit notamment des «données relatives au contenu», comme les courriels, les SMS ou textos, les photos et les vidéos, ainsi que les «données non relatives au contenu», comme les données relatives aux abonnés ou les informations sur le trafic concernant un compte en ligne.

La coopération entre les autorités judiciaires est la méthode classique que les autorités emploient pour collaborer à la lutte contre tous types d'infractions. Aujourd'hui, le principal instrument utilisé par les États membres pour demander l'accès à des preuves électroniques transfrontières dans la plupart des autres pays de l'Union européenne est la décision d'enquête européenne.

Les États membres de l'Union européenne ont recours aux demandes d'entraide judiciaire avec les pays tiers (ainsi que le Danemark et l'Irlande, qui ne participent pas au mécanisme de la décision d'enquête européenne). Plusieurs autorités différentes interviennent des deux côtés. Les procédures ont été mises au point avant l'avènement de l'internet, à une époque où les volumes de demandes étaient minimes par rapport à ceux d'aujourd'hui, et où le problème inhérent à la nature volatile des preuves électroniques ne se posait pas.

Les États-Unis d'Amérique, où les plus grands fournisseurs de services ont leur siège, sont l'un des principaux destinataires des demandes d'entraide judiciaire émanant des États membres de l'Union européenne (et des pays du monde entier) et visant à obtenir l'accès à des preuves électroniques. Un accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire a été signé le 25 juin 2003 et est entré en vigueur le 1er février 2010. Cet accord constitue un mécanisme transatlantique essentiel pour garantir une coopération efficace dans le domaine de la justice pénale et combattre la criminalité organisée et le terrorisme.

Un premier réexamen conjoint de l'accord a eu lieu en 2016[1]. Il en est ressorti que l'accord conférait une valeur ajoutée à la relation entre l'UE et les États-Unis en matière d'entraide judiciaire et fonctionnait bien de manière générale. Des efforts supplémentaires seront consentis pour améliorer cette coopération. Bien que la coopération judiciaire entre les autorités publiques, y compris avec celles des États-Unis d'Amérique, soit essentielle, cette méthode, dont la durée moyenne est de 10 mois, est souvent trop lente eu égard à la nature volatile des preuves électroniques et peut entraîner une dépense de ressources disproportionnée. En outre, alors que la souveraineté est un aspect important de la coopération judiciaire dans une enquête donnée, il devient de plus en plus fréquent que le seul lien avec un autre État soit la localisation des données ou du fournisseur de services. En ce qui concerne les preuves électroniques en particulier, le réexamen conjoint de 2016 a encouragé les États membres à coopérer directement avec les fournisseurs de services américains afin de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement.

La coopération directe avec les fournisseurs de services américains est devenue une voie alternative à la coopération judiciaire. Elle est limitée aux données non relatives au contenu[2] et se fait sur une base volontaire du point de vue de la législation américaine. Concrètement, les autorités publiques de l'État membre concerné de l'Union européenne s'adressent directement à un fournisseur de services établi aux États-Unis d'Amérique en lui soumettant une demande conforme aux règles nationales de procédure pénale concernant des données auxquelles le fournisseur a accès, généralement des données relatives à un utilisateur des services qu'il fournit. Sont concernés certains fournisseurs de services établis aux États-Unis d'Amérique et, dans une moindre mesure, en Irlande, qui répondent directement aux demandes émanant des autorités répressives des États membres sur une base volontaire, dans la mesure où ces demandes portent sur des données non relatives au contenu.

La législation américaine[3] permet aux fournisseurs de services établis aux États-Unis d'Amérique de coopérer directement avec des autorités publiques européennes dans le cas de données non relatives au contenu. Cette coopération a toutefois lieu sur une base volontaire. En conséquence, les fournisseurs ont établi leurs propres politiques ou se prononcent au cas par cas sur l'opportunité de coopérer et, le cas échéant, sur le mode de coopération. Outre le recours accru à une coopération directe avec les fournisseurs de services, de récentes décisions et affaires judiciaires aux États-Unis d'Amérique ont tenté de préciser si les autorités américaines avaient le droit de demander la production de données stockées à l'étranger par un fournisseur de services dont le siège principal est établi aux États-Unis d'Amérique, notamment et en particulier dans l'affaire «Microsoft Ireland»[4].

Le volume des demandes de coopération directe sur une base volontaire a augmenté rapidement, pour dépasser le nombre de 124 000 en 2017. Bien qu'elle garantisse un accès plus rapide par rapport à la demande d'entraide judiciaire, la coopération directe sur une base volontaire est limitée aux données non relatives au contenu. En outre, elle n'est pas toujours fiable, n'assure pas nécessairement le respect des garanties procédurales appropriées, n'est

---

1 Réexamen de l'accord UE – États-Unis en matière d'entraide judiciaire de 2010, 7 avril 2016, 7403/16.

2 Les données relatives au contenu peuvent être obtenues uniquement sur une base volontaire dans les cas considérés comme une urgence comportant un danger de mort ou le risque de lésions corporelles graves pour une personne.

3 Article 2701(2) de l'«Electronic Communications Privacy Act 1986 (ECPA)» (loi sur la confidentialité des communications électroniques de 1986).

4 L'affaire a été examinée par la Cour suprême américaine le 27 février 2018. La Cour a classé l'affaire le 17 avril 2018, après avoir été informée par les parties de la promulgation du «CLOUD Act», qui autorisait l'émission d'une nouvelle ordonnance permettant d'obtenir des informations auprès de Microsoft.

possible qu'avec un nombre limité de fournisseurs de services appliquant tous leurs propres politiques, n'est pas transparente et ne comporte pas d'obligation de rendre compte. La fragmentation qui en résulte peut être source d'insécurité juridique, soulever des questions quant à la légalité des poursuites ainsi que des préoccupations concernant la protection des droits fondamentaux et des garanties procédurales pour les personnes concernées par ces demandes. En outre, sur l'ensemble des demandes adressées aux fournisseurs de services, moins de la moitié sont satisfaites[5].

En ce qui concerne de possibles demandes réciproques adressées par des autorités américaines à des fournisseurs de services établis dans l'Union européenne, dans bon nombre d'États membres, le cadre juridique des télécommunications interdit actuellement aux fournisseurs de télécommunications nationaux de répondre directement aux demandes émanant d'autorités étrangères, y compris pour des données non relatives au contenu. En outre, il n'existe aucun cadre juridique permettant une coopération directe dans d'autres secteurs des communications. Les autorités américaines ne peuvent généralement obtenir ce type de données auprès de fournisseurs de services de l'UE que dans le cadre d'une demande d'entraide judiciaire.

2. OBJECTIFS DE LA PROPOSITION

La Commission européenne s'est engagée, dans le programme européen en matière de sécurité d'avril 2015[6], à faire le point sur les obstacles aux enquêtes pénales sur des infractions facilitées par l'internet, notamment en ce qui concerne l'accès transfrontière aux preuves électroniques. Le 17 avril 2018, la Commission a proposé au Parlement européen et au Conseil un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[7] et une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale (les «propositions relatives aux preuves électroniques»)[8].

Ces propositions ont pour objet d'accélérer, dans l'Union européenne, le processus permettant de recueillir et d'obtenir des preuves électroniques directement auprès de fournisseurs de services établis dans une autre juridiction. Le champ d'application des propositions englobe des types de fournisseurs particuliers qui offrent leurs services 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. Ceux qui ne sont pas présents dans l'Union européenne sont tenus de désigner un représentant légal à l'égard duquel des injonctions de production peuvent être exécutées.

---

5 Commission Impact Assessment accompanying the e-evidence package (analyse d'impact de la Commission accompagnant le train de mesures concernant les preuves électroniques), 17 avril 2018, SWD(2018) 118 final.

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

7 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.

8 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.

Le Conseil européen a souligné l'importance de cette question sur le plan tant intérieur qu'extérieur. Selon les conclusions du Conseil européen du 18 octobre 2018, «*[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*[9]*. 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 jettent les bases d'une approche coordonnée et cohérente applicable par l'Union européenne tant en son sein qu'au niveau international, dans le respect des règles de l'Union européenne, notamment en matière de non-discrimination entre les États membres et leurs ressortissants. Alors que la Commission a déjà fait observer dans son analyse d'impact concernant les propositions relatives aux preuves électroniques que ces dernières pourraient être utilement complétées par des accords bilatéraux ou multilatéraux en matière d'accès aux preuves électroniques assortis des garanties nécessaires, elle a décidé de proposer des règles de l'UE relatives aux modalités et garanties appropriées concernant l'accès transfrontière aux preuves électroniques, avant d'entamer des négociations avec des tiers.

Au niveau international, les discussions se tiennent dans le cadre des négociations relatives à un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe[10]. L'accès transfrontière aux preuves électroniques a été abordé régulièrement lors des dernières réunions ministérielles entre l'UE et les États-Unis dans le domaine de la justice et des affaires intérieures.

Les deux recommandations concernant l'ouverture de négociations avec les États-Unis d'Amérique et la participation aux négociations sur le deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe sont en cours d'adoption simultanée par la Commission. Les deux processus progresseront certes à un rythme différent, mais ils abordent des questions étroitement liées et les engagements pris au cours d'une négociation peuvent avoir une incidence directe sur d'autres axes de négociation.

Alors que les propositions relatives aux preuves électroniques abordent la situation de certains types de fournisseurs proposant leurs services sur le marché de l'Union, le risque existe de voir apparaître des obligations contradictoires avec les législations de pays tiers. Pour éviter ces conflits de lois, et conformément au principe de courtoisie internationale, les propositions relatives aux preuves électroniques comportent des mécanismes spécifiques qui s'appliquent lorsqu'un fournisseur de services est confronté, lorsque des preuves lui sont demandées, à des obligations contradictoires découlant de la législation d'un pays tiers. Ces mécanismes comprennent une procédure d'examen permettant de clarifier ce type de situation. Un accord entre l'UE et les États-Unis devrait avoir pour objectif d'éviter l'existence d'obligations contradictoires entre l'Union européenne et les États-Unis d'Amérique.

---

9 Alors que les négociations avec le Parlement européen et le Conseil se poursuivent, ce dernier a arrêté une orientation générale concernant la proposition de règlement de la Commission lors du Conseil «Justice et affaires intérieures» du 7 décembre 2018.

10 Convention de Budapest sur la cybercriminalité du Conseil de l'Europe (STCE n° 185), 23 novembre 2001, http://conventions.coe.int

De grands fournisseurs de services détenant des preuves pertinentes pour des enquêtes pénales exercent leurs activités sous la juridiction des États-Unis. Le «Stored Communications Act» (loi sur les communications stockées) de 1986 a interdit la divulgation de données relatives au contenu, tandis que les données non relatives au contenu peuvent être fournies sur une base volontaire. Le CLOUD (Clarifying Lawful Overseas Use of Data) Act (loi visant à clarifier l'utilisation légale des données à l'étranger) adopté par le Congrès américain le 23 mars 2018 précise, au moyen d'un amendement au «Stored Communications Act» de 1986, que les fournisseurs de services américains sont tenus de se conformer aux ordonnances américaines prescrivant la divulgation de données relatives ou non relatives au contenu, quel que soit l'endroit où ces données sont stockées, y compris dans l'Union européenne. Le «CLOUD Act» permet également la conclusion d'accords exécutifs avec des gouvernements étrangers, sur la base desquels les fournisseurs de services américains seraient en mesure de fournir des données relatives au contenu directement à ces gouvernements étrangers. Le champ d'application du «CLOUD Act» relatif aux données englobe les données stockées et l'interception de communications électroniques ou par fil, tandis que le champ d'application relatif aux infractions recouvre les «infractions graves». Les accords exécutifs conclus avec des gouvernements étrangers sont soumis à certaines conditions garantissant que le pays étranger dispose de protections suffisantes, notamment pour restreindre l'accès aux données relatives à des citoyens américains.

La présente initiative a pour objet de traiter, au moyen de règles communes, la question juridique spécifique de l'accès aux données relatives ou non relatives au contenu détenues par des fournisseurs de services dans l'Union européenne et aux États-Unis d'Amérique. Dans le contexte d'un accord international, elle compléterait les propositions de l'Union relatives aux preuves électroniques en remédiant aux conflits de lois, en particulier en ce qui concerne les données relatives au contenu, et en accélérant l'accès aux preuves électroniques. La présente recommandation comprend des directives de négociation pour l'ouverture de négociations sur un accord à l'échelle de l'UE avec les États-Unis d'Amérique en ce qui concerne l'accès transfrontière aux preuves électroniques. Il est dans l'intérêt de l'Union européenne de conclure un accord global avec les États-Unis d'Amérique, tant pour protéger les droits et valeurs européens, tels que le respect de la vie privée et la protection des données à caractère personnel, que pour préserver ses propres intérêts en matière de sécurité.

En ce qui concerne les données relatives au contenu, comme cela a été souligné plus haut, la législation américaine (le «Stored Communications Act» de 1986) sous sa forme actuelle interdit aux fournisseurs de services américains de répondre aux demandes émanant d'autorités répressives étrangères. La législation américaine exige l'invocation d'un motif raisonnable avant l'exécution d'une demande d'entraide judiciaire émanant d'un pays tiers. Les fournisseurs de services des États membres de l'Union européenne ne peuvent actuellement répondre aux demandes directes qui leur sont adressées par les autorités de pays tiers. Un accord entre l'UE et les États-Unis compléterait l'objectif et l'efficacité des propositions relatives aux preuves électroniques, en particulier pour les données relatives au contenu détenues par des fournisseurs de services américains aux États-Unis d'Amérique. Il permettrait une coopération directe avec un fournisseur de services en établissant un cadre juridique plus efficace pour les autorités judiciaires, car les praticiens de l'Union rencontrent actuellement des difficultés pour obtenir des données relatives au contenu dans le cadre de demandes d'entraide judiciaire.

S'agissant des données non relatives au contenu, compte tenu du nombre croissant de demandes d'entraide judiciaire adressées aux États-Unis d'Amérique, les autorités américaines ont encouragé les autorités répressives et judiciaires de l'UE à demander directement aux fournisseurs de services américains de leur fournir ce type de données, et la

législation américaine autorise les fournisseurs de services établis aux États-Unis à répondre à ces demandes, sans les y contraindre pour autant. Un accord entre l'UE et les États-Unis offrirait une sécurité accrue et des garanties procédurales claires et réduirait la fragmentation à laquelle les autorités de l'Union sont confrontées pour accéder à des données non relatives au contenu détenues par des fournisseurs de services américains. Il permettrait également un accès réciproque des autorités américaines aux données détenues par des fournisseurs de services de l'UE.

La recommandation de décision du Conseil a pour objet l'ouverture de négociations entre l'Union européenne et les États-Unis d'Amérique, en vue de parvenir à un accord transatlantique garantissant la possibilité d'obtenir, aux fins de procédures pénales, un accès transfrontière aux preuves électroniques directement auprès de fournisseurs de services. Elle vise à adapter les mécanismes de coopération à l'ère numérique en fournissant les outils judiciaires et répressifs nécessaires pour tenir compte des modes de communication actuels des criminels et pour lutter contre les formes modernes de criminalité.

Un accord entre l'Union européenne et les États-Unis offrirait plusieurs avantages concrets:

- il garantirait un accès réciproque des autorités judiciaires aux données relatives au contenu;
- il traiterait la question de l'accès aux données non relatives au contenu sur la base d'injonctions d'autorités judiciaires, garantirait l'accès réciproque des autorités américaines et de l'UE et permettrait de réexaminer les conditions et garanties d'une coopération directe avec des fournisseurs de services;
- il contribuerait à accélérer l'accès des autorités judiciaires aux données;
- il remédierait au risque de conflit de lois;
- il réduirait le risque de fragmentation des règles et procédures et harmoniserait les droits et les garanties au moyen d'un mandat de négociation avec les États-Unis unique pour tous les États membres de l'Union européenne qui assure le respect du principe de non-discrimination entre les États membres de l'Union européenne et leurs ressortissants;
- il clarifierait le caractère contraignant et les modalités d'exécution des injonctions adressées aux fournisseurs de services, tout en détaillant les obligations incombant aux autorités judiciaires.

L'accord devrait être subordonné à la mise en place de solides mécanismes de protection des droits fondamentaux. Les présentes directives de négociation visent à améliorer la sécurité juridique au profit des autorités, des fournisseurs de services et des personnes concernées, en garantissant la proportionnalité, la protection des droits fondamentaux, la transparence et l'obligation de rendre compte incombant tant aux autorités judiciaires qu'aux fournisseurs de services.

3. DISPOSITIONS EXISTANTES DANS LE DOMAINE D'ACTION

Le cadre juridique actuel de l'Union européenne se compose des instruments de coopération de l'Union en matière pénale, tels que la directive 2014/41/UE concernant la décision

d'enquête européenne en matière pénale[11], la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[12], le règlement 2018/1727 instituant Eurojust[13], le règlement (UE) 2016/794 relatif à Europol[14], la décision-cadre 2002/465/JAI du Conseil relative aux équipes communes d'enquête[15] et la proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne[16].

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[17] et une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale[18]. Sur le plan extérieur, l'Union européenne a conclu plusieurs accords bilatéraux entre l'Union et des pays tiers, tels que l'accord en matière d'entraide judiciaire avec les États-Unis d'Amérique[19]. L'accord faisant l'objet de la présente recommandation est destiné à compléter ces arrangements.

Les données à caractère personnel couvertes par la présente recommandation de décision du Conseil sont protégées et ne peuvent être traitées que dans le respect du règlement général sur la protection des données (RGPD)[20] et, pour les autorités au sein de l'Union européenne, de la directive relative à la protection des données destinées aux autorités policières et aux autorités judiciaires pénales (directive relative à la protection des données dans un contexte répressif)[21]. L'accord devrait compléter l'accord UE – États-Unis sur la protection des données et le respect de la vie privée, également connu sous le nom d'«accord-cadre», qui est entré en vigueur le 1er février 2017, et le «Judicial Redress Act» (loi sur le recours juridictionnel)

---

11 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.

12 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.

13 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.

14 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.

15 Décision-cadre 2002/465/JAI du Conseil du 13 juin 2002 relative aux équipes communes d'enquête.

16 Proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, COM(2018) 640 final.

17 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.

18 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.

19 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.

20 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.

21 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.

américain, qui étend aux citoyens de l'UE les avantages du «Privacy Act» (loi sur la protection de la vie privée) américain et a été adopté par le Congrès américain le 24 février 2016.

Les données de communications électroniques couvertes par la présente recommandation de décision du Conseil sont protégées et ne peuvent être traitées que dans le respect de la directive 2002/58/CE (la directive «vie privée et communications électroniques»)[22].

L'accord devrait respecter les libertés et droits fondamentaux et les principes généraux du droit de l'Union tels qu'inscrits dans les traités et la charte des droits fondamentaux de l'Union européenne, les droits procéduraux, y compris le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité des délits et des peines, et toute obligation qui incombe aux autorités répressives ou judiciaires à cet égard. En ce qui concerne les garanties nécessaires en matière de protection des données pour les données à caractère personnel transférées de l'Union européenne à des autorités répressives américaines, les dispositions applicables de l'accord UE – États-Unis sur la protection des données et le respect de la vie privée seront complétées par des garanties supplémentaires afin de tenir compte du niveau de sensibilité des catégories de données concernées et des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services.

L'accord devrait également être sans préjudice d'autres accords internationaux existants dans le domaine de la coopération judiciaire en matière pénale entre autorités, tels que l'accord UE – États-Unis en matière d'entraide judiciaire. L'accord devrait, dans le cadre des relations bilatérales entre les États-Unis d'Amérique et l'Union européenne, prévaloir sur tout accord ou arrangement conclu lors des négociations concernant le deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe.

Le Conseil autorise l'ouverture de négociations, adopte des directives de négociation et autorise la signature et la conclusion de l'accord conformément à l'article 218, paragraphes 3 et 4, du traité sur le fonctionnement de l'Union européenne.

Droits fondamentaux

L'accord serait susceptible de porter atteinte à plusieurs droits fondamentaux:

- les droits des personnes dont les données sont consultées: y compris le droit à la protection des données à caractère personnel; le droit au respect de la vie privée et familiale, du domicile et des communications; le droit à la liberté d'expression et de réunion; le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité des délits et des peines;

[22] 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 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) n° 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.

- les droits du fournisseur de services: le droit à la liberté d'entreprise; le droit à un recours effectif;
- les droits à la liberté et à la sécurité des personnes.

Compte tenu de l'acquis pertinent en matière de respect de la vie privée et de protection des données, il convient d'inclure dans l'accord des garanties suffisantes et importantes afin de veiller à ce que les droits de ces personnes soient protégés conformément aux principes généraux du droit de l'Union et à la jurisprudence applicable de la Cour de justice européenne.

L'accord entre l'UE et les États-Unis devrait être compatible avec les propositions de la Commission relatives aux preuves électroniques, en ce compris leurs évolutions dans le cadre de la procédure législative et sous leur forme définitive adoptée.

Les définitions des procédures pénales aux fins desquelles de telles données pourraient être obtenues, les types de données couverts, les exigences relatives à l'émission d'une injonction, les recours et garanties juridictionnels et la portée des infractions concernées constitueront un volet important des négociations, le but étant d'éviter les conflits de lois et d'améliorer l'accès des autorités. Les définitions et le champ d'application devraient être compatibles avec les définitions et le champ d'application des règles internes de l'UE concernant les preuves électroniques, en ce compris leurs évolutions.

La Commission considère qu'il est dans l'intérêt tant de l'Union européenne que des États-Unis d'Amérique de conclure un accord global, car celui-ci offrirait une sécurité juridique aux autorités judiciaires et répressives des deux parties et éviterait aux fournisseurs de services d'être confrontés à des obligations juridiques contradictoires. Il s'agit également du seul moyen d'éviter que les citoyens et les fournisseurs de services de l'UE ne se voient appliquer des règles différentes selon leur nationalité.

L'accord devrait clarifier le caractère contraignant et les modalités d'exécution des injonctions adressées aux fournisseurs de services, tout en définissant les obligations incombant aux autorités judiciaires.

Aux points 1 à 3 des directives de négociation, la Commission propose les trois principaux objectifs de l'accord, à savoir premièrement, fixer des règles communes et prévenir les conflits de lois pour les injonctions concernant des données relatives ou non relatives au contenu, adressées par une autorité judiciaire établie au sein d'une partie contractante à un fournisseur de services soumis au droit d'une autre partie contractante; deuxièmement, sur la base d'une telle injonction, prévoir un transfert de preuves électroniques, direct et sur une base réciproque, d'un fournisseur de services à une autorité requérante; et troisièmement, garantir le respect des libertés et droits fondamentaux et des principes généraux du droit de l'Union tels qu'inscrits dans les traités et la charte des droits fondamentaux de l'Union européenne.

Au point 4 des directives de négociation, la Commission propose que l'accord s'applique aux procédures pénales tant lors de la phase préalable au procès que durant le procès. Il devrait être compatible avec l'article 3 de la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale. Toutes les protections juridiques prévues pour les personnes concernées, et en particulier les garanties procédurales de droit pénal, sont applicables tant lors de la phase préalable au procès que durant le procès.

Avec le point 5 des directives de négociation, la Commission propose que l'accord crée les droits et obligations réciproques des parties à l'accord.

Au point 6 des directives de négociation, la Commission propose que l'accord énonce les définitions et les types de données à couvrir, incluant à la fois les données relatives au contenu et les données non relatives au contenu. Les données relatives au contenu englobent le contenu des échanges électroniques et sont considérées comme la catégorie de preuves électroniques la plus intrusive. Les données non relatives au contenu englobent à la fois les données relatives aux abonnés, qui constituent le type de données le plus fréquemment demandé aux fins d'enquêtes pénales, et les données relatives au trafic, qui incluent les informations sur les identités des expéditeurs et des destinataires de messages électroniques et des métadonnées telles que l'heure, la fréquence et la durée des échanges.

Au point 7 des directives de négociation, la Commission propose que l'accord définisse son champ d'application exact pour ce qui est des infractions pénales couvertes et des seuils des niveaux de sanctions. Il devrait être compatible avec l'article 5, paragraphe 4, de la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale. L'autorité d'émission devrait être tenue de faire en sorte, dans le cas concerné, que la mesure soit nécessaire et proportionnée, y compris au regard de la gravité de l'infraction faisant l'objet de l'enquête. L'accord devrait prévoir des seuils de niveaux de sanctions appropriés pour les données relatives ou non relatives au contenu. Il devrait être compatible avec le seuil de trois ans, qui limite le champ d'application de l'instrument aux infractions plus graves, sans restreindre de façon excessive les possibilités d'utilisation de cet instrument par les praticiens.

La Commission propose au point 8 des directives de négociation que l'accord énonce les conditions à remplir pour qu'une autorité judiciaire puisse émettre une injonction, ainsi que les modalités de signification de l'injonction. Il devrait être compatible avec l'article 5 de la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, qui énonce les conditions d'émission de l'injonction.

Au point 9 des directives de négociation, la Commission propose que l'accord comporte une clause permettant aux suspects et aux personnes poursuivies de former des recours juridictionnels effectifs pendant la procédure pénale. L'accord devrait également définir les circonstances dans lesquelles un fournisseur de services a le droit de s'opposer à une injonction. Pour les personnes concernées, le point de référence pour ces dispositions est l'article 17 de la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, qui assure aux personnes concernées par une injonction européenne de production des recours effectifs conformes au droit national, normalement pendant la procédure pénale. Les recours dont disposent les personnes concernées sont également définis dans la directive (UE) 2016/680 et le règlement (UE) 2016/679. L'injonction étant une mesure contraignante, elle pourrait également porter atteinte aux droits des fournisseurs de services, en particulier la liberté d'entreprise et les conditions y afférentes. La Commission propose que l'accord reconnaisse au fournisseur de services le droit de faire valoir certaines prétentions dans l'État membre d'émission, par exemple dans le cas où l'injonction n'a pas été émise ou validée par une autorité judiciaire.

Au point 10 des directives de négociation, la Commission propose que l'accord définisse le délai dans lequel les données faisant l'objet de l'injonction doivent être fournies. Il devrait être compatible avec l'article 9 de la proposition de règlement relatif aux injonctions

européennes de production et de conservation de preuves électroniques en matière pénale, qui contraint les destinataires à répondre à l'injonction dans un délai normal de 10 jours, les autorités pouvant fixer un délai plus court si cela se justifie.

La Commission propose au point 11 des directives de négociation que l'accord s'applique sans préjudice d'autres accords internationaux existants dans le domaine de la coopération judiciaire en matière pénale entre autorités, tels que l'accord UE – États-Unis en matière d'entraide judiciaire.

Au point 12 des directives de négociation, la Commission propose que, dans le cadre des relations bilatérales entre les États-Unis d'Amérique et l'Union européenne, l'accord prévale sur la convention sur la cybercriminalité du Conseil de l'Europe et sur tout accord ou arrangement conclu à l'issue des négociations concernant le deuxième protocole additionnel à la convention, dans la mesure où les dispositions dudit accord ou arrangement traitent de points abordés par l'accord faisant l'objet de la présente recommandation.

Au point 13 des directives de négociation, la Commission propose que l'accord soit réciproque pour ce qui est des catégories de personnes dont les données ne doivent pas être demandées en vertu de cet accord. L'accord ne devrait pas établir de distinction entre les citoyens des différents États membres de l'Union européenne. La Commission considère que cet accord, qui est applicable à l'échelle de l'UE, garantit le respect de cette exigence de non-discrimination.

Les points 14 à 16 des directives de négociation concernent les garanties en matière de protection des données qui s'imposent pour cet accord particulier. Le point 14 des directives de négociation prévoit que l'accord devrait rendre applicable, en s'y référant, l'accord UE – États-Unis sur la protection des données et le respect de la vie privée, également connu sous le nom d'«accord-cadre». Au point 15, la Commission indique que l'accord devrait compléter l'accord-cadre par des garanties supplémentaires tenant compte du niveau de sensibilité des catégories de données concernées et des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités. Le point 16 définit les garanties supplémentaires que la Commission propose d'intégrer dans l'accord, y compris la spécification de la finalité, la limitation de la finalité, la notification et le transfert ultérieur.

Le point 17 des directives de négociation porte sur les droits procéduraux supplémentaires qui, selon la proposition de la Commission, devraient être prévus pour tenir compte des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités. Il s'agit notamment du fait que les données ne puissent être demandées aux fins d'une procédure pénale susceptible d'aboutir à une condamnation à la peine de mort, de la proportionnalité des injonctions et de garanties spécifiques pour les données protégées par des privilèges ou des immunités. Les immunités et les privilèges liés à certaines professions, par exemple celle d'avocat, ainsi que les intérêts fondamentaux de sécurité ou de défense nationales dans l'État du destinataire doivent aussi être pris en considération lors du procès dans l'État d'émission. L'examen par une autorité judiciaire constitue ici une garantie supplémentaire.

Dans les dispositions relatives à la gouvernance de l'accord figurant aux points 18 à 23 des directives de négociation, la Commission propose que l'accord prévoie des réexamens périodiques conjoints de l'application de l'accord et comporte une clause relative à sa durée. Il est également proposé que l'accord précise que les parties se consultent pour faciliter le

règlement de tout différend concernant l'interprétation ou l'application de l'accord. Les deux parties devraient collecter des statistiques afin de faciliter le processus de réexamen. En outre, les directives de négociation proposent que le futur accord comporte une clause de suspension et de résiliation applicable dans le cas où la procédure de consultation ne permet pas de régler le différend.

Recommandation de

DÉCISION DU CONSEIL

autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale

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,

(1) Le 17 avril 2018, la Commission a présenté au Parlement européen et au Conseil des propositions législatives concernant un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale (les «propositions relatives aux preuves électroniques»)[23]. Le Conseil a arrêté une orientation générale concernant la proposition de la Commission relative au règlement lors du Conseil «Justice et affaires intérieures» du 7 décembre 2018[24].

(2) Il y a lieu d'ouvrir des négociations en vue de la conclusion d'un accord entre l'Union et les États-Unis d'Amérique sur l'accès transfrontière des autorités judiciaires aux preuves électroniques détenues par un fournisseur de services dans le cadre de procédures pénales.

(3) L'accord devrait comporter les garanties propres à assurer la protection des libertés et droits fondamentaux et le respect des principes reconnus par la charte des droits fondamentaux de l'Union européenne, en particulier 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 l'accord soit appliqué conformément à ces droits et principes,

[23] 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 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.

[24] Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale – orientation générale du Conseil, ST 15292 2018 INIT, 12 décembre 2018.

(4) 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 européen et du Conseil[25] et a rendu un avis le ...[26],

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La Commission est autorisée à négocier, au nom de l'Union, un accord entre l'Union et les États-Unis d'Amérique sur l'accès transfrontière des autorités judiciaires aux preuves électroniques détenues par un fournisseur de services dans le cadre de procédures pénales.

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

[25] 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).

[26] JO C ….