COMMISSION
EUROPÉENNE

Bruxelles, le 5.2.2019
COM(2019) 70 final

ANNEX

ANNEXE

de

la 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

ANNEXE

1. OBJECTIFS

Il convient que la Commission, au cours des négociations, vise à atteindre les objectifs spécifiques énoncés de façon détaillée ci-dessous, tout en veillant à ce que le résultat des négociations soit compatible avec les règles internes de l'Union concernant les preuves électroniques, en ce compris leurs évolutions dans le cadre de la procédure législative menée par les colégislateurs de l'Union et, in fine, sous leur forme définitive adoptée. Ces règles internes serviront de référence pour la position de négociation de l'Union.

1. Fixer des règles communes et prévenir les conflits de lois pour les injonctions concernant l'obtention de preuves électroniques sous la forme de 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 de l'autre partie contractante. Cela devrait réduire le risque de fragmentation des pratiques et des règles juridiques et renforcer la sécurité juridique entre l'Union et les États-Unis d'Amérique lorsqu'il s'agit d'obtenir des preuves électroniques dans le cadre de procédures pénales.

2. Prévoir un transfert de preuves électroniques, direct et sur une base réciproque, d'un fournisseur de services à une autorité requérante, comme indiqué au paragraphe 1.

3. 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, notamment la proportionnalité, les droits procéduraux, la présomption d'innocence et les droits de la défense des personnes faisant l'objet d'une procédure pénale, ainsi que le respect de la vie privée et la protection des données à caractère personnel et des données de communication, lorsque de telles données sont traitées, y compris les transferts aux autorités répressives de pays tiers, et toute obligation qui incombe aux autorités répressives et judiciaires à cet égard.

Pour atteindre les objectifs énoncés dans la section 1, l'accord devrait notamment porter sur les éléments mentionnés ci-après.

2. NATURE ET PORTÉE DE L'ACCORD

4. L'accord devrait s'appliquer aux procédures pénales tant lors de la phase préalable au procès que durant le procès.

5. L'accord devrait créer les droits et obligations réciproques des parties.

6. L'accord devrait énoncer 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.

7. L'accord devrait définir son champ d'application exact pour ce qui est des infractions pénales couvertes et des seuils.

8. L'accord devrait énoncer les conditions à remplir pour qu'une autorité judiciaire puisse émettre une injonction, ainsi que les modalités de signification de l'injonction.

9. L'accord devrait comporter une clause permettant aux personnes concernées 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.

10. L'accord devrait définir le délai dans lequel les données faisant l'objet de l'injonction doivent être fournies.

11. L'accord devrait s'appliquer 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.

12. L'accord devrait, dans le cadre des relations bilatérales entre l'Union et les États-Unis d'Amérique, prévaloir 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 sur la cybercriminalité du Conseil de l'Europe, dans la mesure où les dispositions dudit accord ou arrangement traitent de points abordés par l'accord.

3. GARANTIES

13. L'accord devrait être réciproque pour ce qui est des catégories de personnes dont les données ne doivent pas être demandées en vertu de l'accord. L'accord ne devrait pas établir de distinction entre les citoyens des différents États membres.

14. 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», qui est entré en vigueur le 1er février 2017.

15. 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.

16. Les garanties supplémentaires en matière de respect de la vie privée et de protection des données, à revoir en fonction de la portée de l'accord, devraient notamment comprendre:

(a) la spécification des finalités pour lesquelles des données à caractère personnel et des données de communications électroniques peuvent être demandées et transférées;

(b) l'exigence selon laquelle l'injonction est limitée aux données à caractère personnel et aux données de communications électroniques qui sont nécessaires et proportionnées au regard des finalités pour lesquelles elles sont consultées;

(c) l'exigence selon laquelle la divulgation des données à d'autres autorités américaines non liées par l'accord-cadre et l'utilisation de ces données par lesdites autorités font l'objet d'une notification à, et d'une autorisation préalable de, l'autorité judiciaire compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté, et ne peuvent avoir lieu que s'il est garanti que l'autorité destinataire protège effectivement les données à caractère personnel et les données de communications électroniques conformément aux dispositions de l'accord. Dans le cadre de l'octroi de cette autorisation préalable, l'autorité judiciaire compétente devrait tenir dûment compte de tous les éléments pertinents, notamment la gravité de l'infraction et la finalité pour laquelle les données sont transférées initialement;

(d) l'exigence selon laquelle des transferts ultérieurs vers d'autres pays tiers ne peuvent se faire qu'aux autorités répressives chargées de prévenir, de détecter ou de poursuivre les infractions pénales, y compris le terrorisme, et d'enquêter sur celles-ci et devraient faire l'objet d'une notification à, et d'une autorisation préalable de, l'autorité judiciaire compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté. Dans le cadre de l'octroi de cette autorisation préalable, l'autorité judiciaire compétente devrait tenir compte des éléments mentionnés à l'article 7, paragraphe 2, de l'accord-cadre;

(e) l'accord peut comporter une référence aux circonstances exceptionnelles et aux garanties exigées lorsqu'un transfert ultérieur peut avoir lieu sans autorisation préalable, en cas de menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers;

(f) la notification d'un incident relatif à la sécurité des informations à l'autorité compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté s'effectuera dans les conditions énoncées à l'article 10, paragraphe 2, de l'accord-cadre.

17. Les garanties supplémentaires en matière de droits procéduraux, à revoir en fonction de la portée de l'accord, devraient notamment comprendre:

(a) les garanties propres à faire en sorte que les données ne puissent être demandées aux fins d'une procédure pénale susceptible d'aboutir à une condamnation à la peine de mort;

(b) les conditions adéquates pour garantir la nécessité et la proportionnalité des injonctions émises en vue d'obtenir un accès à des preuves électroniques, une distinction étant notamment établie entre les catégories de données, le cas échéant;

(c) les garanties procédurales dont disposent les personnes soumises à une injonction portant sur des données dans le cadre d'une procédure pénale;

(d) les garanties spécifiques pour les données protégées par des privilèges ou des immunités;

(e) les garanties de confidentialité dont jouissent les autorités et les fournisseurs de services, y compris les exigences de non-divulgation.

4. GOUVERNANCE DE L'ACCORD

18. L'accord devrait prévoir que les parties procéderont à des réexamens périodiques conjoints de l'application de l'accord et examineront comment faire une utilisation aussi efficace que possible de ce dernier. À cette fin, les deux parties devraient collecter des statistiques afin de faciliter le processus.

19. L'accord devrait comporter une clause relative à sa durée. Il conviendra d'apprécier à la lumière des résultats des négociations si cette durée doit être indéterminée ou déterminée. Dans un cas comme dans l'autre, il faudrait inclure une disposition exigeant un réexamen de l'accord en temps utile.

20. L'accord devrait préciser que les parties se consulteront pour faciliter le règlement de tout différend concernant l'interprétation ou l'application de l'accord.

21. L’accord devrait prévoir la possibilité d’une suspension ou d’une résiliation de l’accord par l’une ou l’autre partie dans le cas où la procédure de consultation précitée ne permet pas de régler le différend.

22. L’accord devrait comporter une clause relative à son application territoriale.

23. L’accord devrait faire également foi dans toutes les langues officielles de l’Union.