

Bruxelles, le 5.2.2019
COM(2019) 71 final

ANNEX

ANNEXE

de la

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)

ANNEXE

1. OBJECTIFS

Il convient qu'au cours des négociations, la Commission vise à atteindre les objectifs expliqués en détail ci-dessous:

- (a) Les négociations devraient assurer l'entière compatibilité de la convention et des protocoles additionnels avec le droit de l'UE et les obligations qui incombent aux États membres en vertu de celui-ci, notamment en ce qui concerne les pouvoirs d'investigation accordés aux parties non membres de l'Union.
- (b) En particulier, les négociations devraient garantir le respect des droits fondamentaux, des libertés et des principes généraux prévus dans le droit de l'Union, tels qu'ils sont consacrés dans les traités et la charte des droits fondamentaux de l'Union européenne, y compris 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, la protection des données à caractère personnel et des données de communications électroniques lorsqu'elles font l'objet d'un traitement, notamment le transfert aux services répressifs de pays non membres de l'Union européenne, et toute obligation qui incombe aux autorités répressives ou judiciaires à cet égard.
- (c) De plus, le deuxième protocole additionnel devrait être compatible avec les propositions législatives de la Commission relatives aux preuves électroniques, y compris à mesure qu'elles évoluent au cours des négociations entre les colégislateurs dans le cadre de la procédure législative et finalement sous leur forme définitive (adoptée), et prévenir les conflits de lois. Ce protocole devrait notamment, dans toute la mesure du possible, réduire les risques que les injonctions de production émises au titre d'un futur instrument de l'UE créent des conflits avec les législations de pays tiers parties audit protocole additionnel. Assorti de garanties appropriées en matière de protection des données et de la vie privée, il facilitera le 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 deuxième protocole additionnel exigeant qu'un responsable du traitement ou un sous-traitant communique des données à caractère personnel ou des données de communications électroniques.

2. QUESTIONS SPÉCIFIQUES

I. Relation avec le droit de l'Union et d'autres accords (possibles)

- (d) Il convient de veiller à ce que le deuxième protocole additionnel comporte une clause de déconnexion permettant aux États membres de continuer à appliquer les règles de l'Union européenne dans leurs relations mutuelles, plutôt que le deuxième protocole additionnel.
- (e) Le deuxième protocole additionnel peut s'appliquer en l'absence d'autres accords internationaux plus spécifiques qui lient l'Union européenne ou ses États membres et d'autres parties à la convention, ou, si de tels accords internationaux existent, uniquement dans la mesure où certaines questions ne sont pas régies par ceux-ci. Ces accords internationaux plus spécifiques devraient donc prévaloir sur le deuxième

protocole additionnel dès lors qu'ils sont compatibles avec les objectifs et les principes de la convention.

II. Dispositions pour une entraide juridique plus efficace

- (f) Les dispositions sur «la langue dans laquelle doit être formulée une demande» dans leur libellé actuel prévoient que les demandes devraient être adressées dans une langue acceptée par la partie requise ou accompagnées d'une traduction dans une telle langue. L'Union européenne devrait apporter son soutien au projet de texte et au rapport explicatif qui ont fait l'objet d'une adoption préliminaire.
- (g) Les dispositions sur «les procédures d'urgence pour les demandes d'entraide» dans leur libellé actuel permettent de demander une entraide de manière accélérée en envoyant la demande sous forme électronique lorsque la partie requérante estime qu'une urgence existe, en ce sens qu'il y a un danger significatif et imminent pour la vie ou la sécurité d'une personne physique, quelle qu'elle soit. L'Union européenne devrait apporter son soutien au projet de texte et au rapport explicatif qui ont fait l'objet d'une adoption préliminaire. Le champ d'application de l'entraide devrait être identique à celui figurant à l'article 25 de la convention.
- (h) S'agissant des dispositions sur la «vidéoconférence», l'Union européenne devrait faire en sorte que le deuxième protocole additionnel soit conforme aux dispositions correspondantes des accords internationaux en vigueur entre l'Union européenne et ses États membres et d'autres parties à la convention, dans la mesure du possible. Ces dispositions devraient permettre aux États membres d'assurer le respect des garanties applicables en matière de droits procéduraux en vertu du droit de l'Union et du droit national.
- (i) Quant aux dispositions sur «le modèle d'approbation», l'Union européenne devrait œuvrer pour que le projet de texte et l'exposé des motifs contiennent des éléments tels que des délais maximaux contraignants pour les décisions des autorités nationales, afin que l'utilisation de ce modèle accélère les procédures. De plus, ces dispositions devraient garantir que la charge pesant sur les fournisseurs de services est proportionnée et que les voies de recours, le cas échéant, s'appliquent.

III. Dispositions permettant la coopération directe avec des fournisseurs de services dans d'autres juridictions

- (j) L'Union européenne devrait veiller à ce que le deuxième protocole additionnel, dans ses dispositions sur «la coopération directe avec des fournisseurs de services d'autres juridictions», soit conforme au droit de l'Union, contienne les garanties appropriées et prévoie une charge proportionnée pour les fournisseurs de services.
- (k) Elle devrait s'assurer, quant aux dispositions sur «les injonctions de produire internationales», que le deuxième protocole additionnel comporte des garanties appropriées en matière de droits fondamentaux, tenant compte des différents degrés de sensibilité des catégories de données concernées et des garanties prévues dans les injonctions européennes de production pour les différentes catégories de données.
- (l) S'agissant de ces dispositions, l'Union européenne ne devrait pas s'opposer à l'ajout dans le deuxième protocole additionnel de garanties et motifs de refus par rapport aux propositions de la Commission relatives aux preuves électroniques, y compris à mesure qu'elles évoluent au cours des négociations entre les colégislateurs dans le cadre de la procédure législative et finalement sous leur forme définitive (adoptée): par exemple, lesdites dispositions pourraient prévoir une notification ou une approbation par l'État du fournisseur de services et un contrôle préalable effectué

soit par une juridiction, soit par une entité administrative indépendante, tant que cela ne réduit pas de manière disproportionnée l'efficacité de l'instrument prévu dans le deuxième protocole additionnel (par exemple, dans des cas d'urgence dûment justifiés). Les garanties ou motifs de refus supplémentaires ne devraient pas affecter le fonctionnement des propositions de l'UE relatives aux preuves électroniques entre les États membres.

IV. Garanties plus fortes concernant les pratiques existantes en matière d'accès transfrontière aux données

- (m) L'Union européenne devrait s'assurer que les dispositions du deuxième protocole additionnel sur «l'extension des recherches et l'accès sur la base des pouvoirs» et sur les «techniques d'enquête» contiennent des garanties appropriées en matière de droits fondamentaux. Dès lors, il convient que le projet de texte prévoie aussi que les données conservées dans le système informatique connecté soient légalement accessibles à partir du système initial, que l'accès soit nécessaire et proportionné et qu'il ne signifie pas une violation des dispositifs de sécurité des équipements conformément aux garanties décrites plus bas.
- (n) L'Union européenne devrait également veiller à ne pas restreindre les possibilités d'un tel accès qui sont actuellement prévues dans les États membres.

V. Garanties, notamment des conditions relatives à la protection des données

- (o) L'Union européenne veille à ce que le deuxième protocole additionnel prévoie des garanties appropriées en matière de protection des données au sens de la directive (UE) 2016/680, du règlement (UE) 2016/679 et de la directive 2002/58/CE pour la collecte, le transfert et l'utilisation ultérieure des données à caractère personnel et des données de communications électroniques figurant dans les preuves électroniques demandées par l'autorité requérante. Ces garanties devraient être intégrées dans le deuxième protocole additionnel, en tenant compte de celles figurant dans les accords de l'UE, comme l'accord-cadre UE-États-Unis, et dans la convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108). Elles devraient concerner le traitement de données dans le cadre de l'entraide entre les services répressifs et de la coopération directe entre les services répressifs et les fournisseurs. L'Union européenne devrait avoir pour objectif que ces garanties s'appliquent à tous les pouvoirs d'investigation, que ceux-ci existent dans le cadre de la convention ou qu'ils soient instaurés par le deuxième protocole additionnel.

3. APPLICATION TERRITORIALE, ENTRÉE EN VIGUEUR ET AUTRES DISPOSITIONS FINALES

Les dispositions finales du protocole additionnel, notamment les dispositions concernant l'entrée en vigueur, les réserves, la dénonciation, etc., devraient être établies selon le modèle des dispositions de la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185), dans la mesure du possible et s'il y a lieu. Des dispositions s'écartant des clauses types devraient uniquement être utilisées si elles sont nécessaires pour atteindre les objectifs ou refléter les circonstances particulières du deuxième protocole additionnel.