Conseil de
l'Union européenne

Bruxelles, le 1er avril 2022
(OR. fr)

7860/22
ADD 1

CYBER 108
COPEN 118
JAI 444
COPS 143
RELEX 429
JAIEX 30
TELECOM 138
POLMIL 82
CFSP/PESC 432
ENFOPOL 179
DATAPROTECT 95

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	29 mars 2022
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2022) 132 final
Objet:	ANNEXE de la Recommandation de décision du Conseil autorisant les négociations en vue d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Les délégations trouveront ci-joint le document COM(2022) 132 final.

p.j.: COM(2022) 132 final

COMMISSION
EUROPÉENNE

Bruxelles, le 29.3.2022
COM(2022) 132 final

ANNEX

ANNEXE

de la

Recommandation de décision du Conseil

autorisant les négociations en vue d'une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

ANNEXE

En ce qui concerne le déroulement des négociations, l'Union devrait viser les résultats suivants:

(1) Le processus de négociation est ouvert, inclusif et transparent et repose sur une coopération de bonne foi.

(2) Le processus de négociation favorise la participation constructive de l'ensemble des parties prenantes concernées, y compris la société civile, le secteur privé, les milieux universitaires et les organisations non gouvernementales.

(3) Toutes les contributions apportées par l'ensemble des membres des Nations unies sont examinées sur un pied d'égalité, de façon à garantir un processus inclusif.

(4) Le processus de négociation repose sur un programme de travail efficace et réaliste.

En ce qui concerne les objectifs généraux des négociations, l'Union devrait viser les résultats suivants:

(5) La convention sert d'instrument efficace aux services répressifs et aux autorités judiciaires en matière pénale dans la lutte mondiale contre la cybercriminalité, dans le but d'apporter de la valeur ajoutée à la coopération internationale.

(6) Le cadre existant d'instruments internationaux et régionaux ayant fait leurs preuves ainsi que les efforts actuellement déployés, consignés dans les résolutions 74/247 et 75/282 de l'Assemblée générale des Nations unies, sont pleinement pris en considération. Dès lors, la convention est compatible avec les instruments internationaux existants, en particulier la convention de Budapest du Conseil de l'Europe de 2001 sur la cybercriminalité et ses protocoles, la convention des Nations unies de 2000 contre la criminalité transnationale organisée et ses protocoles, mais aussi avec les autres instruments internationaux et régionaux pertinents, et elle les complète. La convention évite toute incidence sur l'application de ces instruments ou sur l'adhésion ultérieure de tout pays à ces derniers et, dans la mesure du possible, évite les redondances.

(7) Comme indiqué dans la résolution 75/282 de l'Assemblée générale des Nations unies, les travaux menés et les résultats obtenus par le groupe intergouvernemental d'experts à composition non limitée chargé de réaliser une étude approfondie sur la cybercriminalité sont pleinement pris en considération.

(8) Les dispositions de la convention offrent la protection des droits de l'homme la plus élevée possible. Les États membres de l'UE devraient être en mesure de se conformer au droit de l'UE, y compris aux droits fondamentaux, aux libertés et aux principes généraux du droit de l'UE tels qu'ils sont consacrés dans les traités européens et dans la charte des droits fondamentaux. Les dispositions de la convention devraient également être compatibles avec les obligations commerciales internationales de l'UE et de ses États membres.

En ce qui concerne le fond des négociations, l'Union devrait viser les résultats suivants:

(9) La convention prévoit la définition des infractions qui ne peuvent être commises qu'au moyen de systèmes d'information.

(10) La convention prévoit la définition des infractions qui peuvent être commises sans recours aux systèmes d'information mais qui, dans certaines circonstances, peuvent être facilitées par l'utilisation desdits systèmes, mais uniquement lorsque la mobilisation de systèmes d'information modifie substantiellement les caractéristiques ou l'effet des infractions.

(11) Les infractions sont définies clairement, strictement et de manière neutre sur le plan technologique. Les définitions sont compatibles avec celles figurant dans les autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité, ainsi qu'avec les normes internationales en matière de droits de l'homme.

(12) La convention prévoit des règles sur la tentative et la complicité commises en vue de la perpétration de telles infractions et sur la responsabilité des personnes morales pour de telles infractions ainsi que des règles sur l'établissement de la compétence à l'égard de ces infractions et sur les sanctions et mesures relatives à ces infractions qui soient compatibles avec les autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité, et avec les normes internationales en matière de droits de l'homme.

(13) La convention prévoit des mesures de procédure pénale qui permettent aux autorités d'enquêter efficacement sur les infractions cybercriminelles, de geler et de confisquer les produits de ces infractions et de conserver ou d'obtenir des preuves électroniques de toute infraction pénale dans le cadre d'une enquête ou d'une procédure pénales, tout en tenant dûment compte du principe de proportionnalité.

(14) Ces mesures de procédure pénale apportent une valeur ajoutée suffisante par rapport aux autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité, et elles sont compatibles avec ces conventions et avec les normes internationales en matière de droits de l'homme.

(15) Les mesures procédurales visant à conserver ou à obtenir des preuves électroniques contiennent une définition claire et stricte du type d'informations visées. Par les mesures procédurales de coopération avec les entités du secteur privé, il est fait en sorte que la charge pesant sur des entités de ce type soit proportionnée et à ce que ces dernières respectent pleinement les droits de l'homme de leurs utilisateurs. La convention clarifie la situation juridique des fournisseurs de services en ligne (par exemple, les fournisseurs de services internet) dans leurs interactions avec les services répressifs des États parties à la convention. Les mesures procédurales encadrant la suppression des contenus illicites ne se rapportent qu'aux contenus illicites qui peuvent être suffisamment concrets et strictement définis.

(16) La convention prévoit des mesures de coopération qui permettent aux autorités des différents États parties à l'instrument de coopérer efficacement aux fins d'enquêtes ou de procédures pénales concernant des infractions définies dans l'instrument ou de coopérer afin de conserver ou d'obtenir des preuves électroniques de toute infraction pénale dans le cadre d'une enquête ou d'une procédure pénales.

(17) Ces mesures de coopération apportent une valeur ajoutée suffisante par rapport aux autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité, et elles sont compatibles avec ces conventions et avec les normes internationales en matière de droits de l'homme.

(18) Les mesures de coopération sont soumises aux conditions prévues par le droit de la Partie requise et prévoient des motifs de refus étendus de nature à garantir la protection des droits fondamentaux, dont le droit à la protection des données à caractère personnel, y compris dans le contexte des transferts de données à caractère personnel, et, s'il y a lieu, l'existence d'une double incrimination.

(19) La convention prévoit des conditions strictes et des garanties solides afin que les États membres de l'UE puissent respecter et protéger les droits fondamentaux, les libertés et les principes généraux du droit de l'UE, tels qu'ils sont consacrés dans les traités européens et la charte des droits fondamentaux, y compris, en particulier, le principe de proportionnalité, les garanties et droits procéduraux, le droit à un recours juridictionnel effectif, la présomption d'innocence, le droit à accéder à un tribunal impartial et les droits de la défense des personnes faisant l'objet d'une procédure pénale, ainsi que le droit à la vie privée, le droit à la protection des données à caractère personnel et des données de communications électroniques lorsque ces données font l'objet d'un traitement, y compris pour les transferts à des autorités situées dans des pays non membres de l'Union européenne, et le droit à la liberté d'expression et d'information. Dans le cadre de la convention, il est fait en sorte notamment que les États membres de l'UE soient en mesure de se conformer aux exigences applicables aux transferts internationaux de données à caractère personnel au sens de la directive (UE) 2016/680, du règlement (UE) 2016/679 et de la directive 2002/58/CE. Ces conditions et garanties permettent également d'assurer la protection des droits de l'homme et des libertés fondamentales conformément aux normes internationales en matière de droits de l'homme. Cela vaut pour l'ensemble de la convention, y compris les mesures procédurales et les mesures de coopération, dont celles qui sont susceptibles de porter considérablement atteinte aux droits des personnes, telles que le gel et la confiscation des produits du crime et l'extradition.

(20) La convention constitue une base pour les mesures volontaires de renforcement des capacités destinées à soutenir les pays dans leur aptitude à mener des enquêtes et procédures efficaces relatives aux infractions cybercriminelles et à obtenir des preuves électroniques aux fins des enquêtes et procédures concernant d'autres infractions, y compris par une assistance technique et des formations. Le rôle dévolu à l'ONUDC pour mettre en œuvre les mesures de cette nature est clairement décrit.

(21) La convention tient dûment compte de la situation des personnes physiques et morales victimes de la cybercriminalité. Par la convention, il est fait en sorte que ces victimes de la cybercriminalité reçoivent une assistance, une aide et une protection appropriées.

(22) La convention constitue une base pour des mesures pratiques de prévention de la cybercriminalité qui soient clairement définies et strictement limitées et distinctes des mesures de procédure pénale qui pourraient porter atteinte aux droits et libertés de personnes physiques ou de personnes morales.

En ce qui concerne le fonctionnement de la convention, l'Union devrait viser les résultats suivants:

(23) La convention préserve les instruments mondiaux et régionaux existants ainsi que la coopération internationale actuelle dans la lutte mondiale contre la cybercriminalité. En particulier, les États membres de l'Union européenne, dans leurs relations mutuelles, sont en mesure de continuer à appliquer les règles de l'Union européenne.

(24) La convention prévoit un mécanisme approprié pour garantir sa mise en œuvre et prévoit des dispositions finales, relatives notamment au règlement des différends, à la signature, à la ratification, à l'acceptation, à l'approbation et à l'adhésion, à l'entrée en vigueur, à l'amendement, à la suspension, à la dénonciation ainsi qu'au dépositaire et aux langues, qui sont inspirées, lorsque cela est possible et approprié, des dispositions des autres conventions internationales ou régionales pertinentes en particulier dans le domaine de la criminalité organisée ou de la cybercriminalité.

(25) La convention permet à l'Union européenne d'y devenir partie.