

COM(2022) 132 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2021/2022

Reçu à la Présidence de l'Assemblée nationale
le 06 avril 2022

Enregistré à la Présidence du Sénat
le 06 avril 2022

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 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

E 16633



Conseil de
l'Union européenne

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

7860/22

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:	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

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**

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

- **Justification et objectifs de la proposition**

D'après l'évaluation de la menace que représente la criminalité organisée sur l'internet¹, la menace que la cybercriminalité fait peser sur la sécurité des citoyens et des entreprises dans l'Union européenne (UE) s'aggrave. La cybercriminalité est un phénomène mondial et sans frontières et, depuis plusieurs années, l'intensification de la coopération internationale dans la lutte contre ce phénomène constitue une priorité pour les pays du monde entier.

La convention du Conseil de l'Europe de 2001 sur la cybercriminalité (la «convention de Budapest») est le premier traité international sur la question; elle définit des infractions liées à la cybercriminalité, prévoit une série de pouvoirs et de procédures pour enquêter sur les actes de cybercriminalité, comme la perquisition de réseaux informatiques et l'interception de données, et pour obtenir des preuves électroniques concernant toute forme de criminalité, et elle instaure un cadre de coopération internationale². La convention de Budapest étant ouverte aux États non membres du Conseil de l'Europe, des pays de toutes les régions du globe y ont adhéré. À ce jour, 66 États y sont parties tandis que quatorze autres pays ont été invités à y adhérer. Cette convention sert de fondement à la législation de lutte contre la cybercriminalité dans 80 % des pays du monde. L'adoption, le 17 novembre 2021 par le Comité des Ministres du Conseil de l'Europe, d'un deuxième protocole additionnel à la convention de Budapest montre que cette convention conserve toute sa pertinence en tant que cadre de coopération internationale en matière de cybercriminalité³.

L'essor des technologies de l'information et le développement rapide de nouveaux systèmes de télécommunications et de réseaux informatiques ainsi que l'utilisation des technologies et leur instrumentalisation à des fins criminelles figurent également parmi les préoccupations des Nations unies. Le 21 décembre 2010, l'Assemblée générale des Nations unies a adopté la résolution 65/230 et prié la Commission pour la prévention du crime et la justice pénale (CPCJP) de créer un groupe intergouvernemental d'experts à composition non limitée (le «GIE») en vue de faire une étude approfondie du phénomène de la cybercriminalité⁴. Lors de sa septième (et dernière) réunion des 6 au 8 avril 2021, le GIE a fait le point sur l'ensemble des conclusions et recommandations préliminaires présentées par les États membres des Nations unies⁵ et il a décidé de transmettre à la CPCJP les 63 conclusions et recommandations

¹ Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2021 www.europol.eu

² Convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest, STE N° 185), 23 novembre 2001, <https://rm.coe.int/168008156d>.

³ [Détails du résultat \(coe.int\).
Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité adopté par le Comité des Ministres du Conseil de l'Europe - News \(coe.int\).](https://rm.coe.int/Le-Deuxieme-Protocole-additionnel-a-la-Convention-sur-la-cybercriminalite-adopté-par-le-Comité-des-Ministres-du-Conseil-de-l-Europe-News-coe.int)

⁴ Résolution de l'Assemblée générale du 21 décembre 2010, <https://www.un.org/fr/ga/65/resolutions.shtml> (undocs.org).

⁵ Compilation de l'ensemble des conclusions et recommandations préliminaires présentées par les États membres lors des réunions du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenues en 2018, 2019 et 2020: [V2101012.pdf \(unodc.org\)](https://www.unodc.org/fr/publications/2021/01/v2101012.pdf).

approuvées⁶. Dans son étude, le GIE n'a pas dégagé de consensus sur la nécessité d'un nouveau traité international en matière de cybercriminalité.

Parallèlement, certains États membres des Nations unies ont intensifié leurs efforts en vue de l'élaboration d'un tel traité dans le cadre des délibérations de la troisième Commission de l'Assemblée générale des Nations unies. L'Assemblée générale des Nations unies a ultérieurement adopté la résolution 73/187 du 17 décembre 2018 intitulée «Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles»⁷. Puis, le 27 décembre 2019, elle a adopté une deuxième résolution, 74/247, sur le même sujet, par laquelle a été établi un comité intergouvernemental spécial d'experts à composition non limitée (le «comité spécial»), ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Cette résolution précisait que le comité spécial devait tenir pleinement compte des instruments internationaux existants et des initiatives déjà prises en la matière aux niveaux national, régional et international, notamment les travaux menés par le GIE et les résultats obtenus par celui-ci⁸. Le 26 mai 2021, l'Assemblée générale des Nations unies a adopté la résolution 75/282 qui a défini les modalités des négociations⁹. Elle a décidé entre autres que le comité spécial tiendrait au moins six sessions, chacune d'une durée de 10 jours, à compter de janvier 2022, ainsi qu'une session de clôture afin de présenter un projet de convention à l'Assemblée générale des Nations unies à sa soixante-dix-huitième session en 2024. Elle a en outre décidé que le comité spécial devrait tenir ses première, troisième et sixième sessions de négociation à New York et les deuxième, quatrième et cinquième sessions à Vienne. Le 20 janvier 2022, l'Assemblée générale a décidé de reporter la première session à une date ultérieure en raison de la situation découlant de la pandémie de COVID-19 à New York.

Par la présente proposition, il s'agit de garantir la participation appropriée de l'Union européenne à ces négociations car ces dernières devraient porter sur des éléments qui concernent la législation et les compétences de l'UE, notamment dans le domaine de la cybercriminalité. L'article 3, paragraphe 2, du traité sur le fonctionnement de l'Union européenne (TFUE) prévoit que l'Union dispose d'une compétence exclusive «pour la conclusion d'un accord international [...] dans la mesure où [cette conclusion] 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.

Étant donné que les négociations portent sur des matières relevant de la compétence de l'Union autres que la politique étrangère et de sécurité commune (PESC), qui devraient constituer les composantes principales de l'accord envisagé, la Commission devrait être désignée chef de l'équipe de négociation. Pour les matières qui concernent la PESC, c'est le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité qui devrait conduire les négociations en tant que membre de l'équipe. Le négociateur en chef de la Commission veillera à la cohérence d'ensemble de l'accord. Sous l'autorité du négociateur en chef, les services de la Commission feront office de chef de file en ce qui concerne les parties de l'accord envisagé qui ne relèveront pas de la PESC et le Service européen pour l'action

⁶ Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 6 au 8 avril 2021: [V2102595.pdf \(unodc.org\)](#).

⁷ Résolution de l'Assemblée générale du 17 décembre 2018, [A/RES/73/187](#).

⁸ Résolution de l'Assemblée générale du 27 décembre 2019, [A/RES/74/247](#).

⁹ Résolution de l'Assemblée générale du 26 mai 2021, [A/RES/75/282*](#).

extérieure (SEAE) assumera le même rôle pour ce qui est des parties de l'accord envisagé qui relèveront de cette matière.

La présente recommandation est présentée au Conseil conformément à l'article 218 du TFUE afin que cette institution autorise les négociations, au nom de l'Union européenne, de la future convention des Nations unies, qu'elle adopte des directives de négociation et qu'elle désigne la Commission en tant que négociateur.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La lutte contre la cybercriminalité est une priorité pour l'Union européenne, comme en témoignent la stratégie pour l'union de la sécurité¹⁰ de 2020 et la stratégie visant à lutter contre la criminalité organisée de 2021¹¹. Dans le troisième rapport sur l'état d'avancement de la mise en œuvre de la stratégie pour l'union de la sécurité publié en 2021, la Commission s'est engagée à veiller à ce que l'Union participe effectivement aux négociations d'une convention internationale générale sur la «lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles» dans le cadre des Nations unies¹².

La Commission reconnaît la nécessité de continuer à faire progresser et à renforcer les capacités des services répressifs et des autorités judiciaires dans ce domaine, ainsi que de développer des réglementations nationales sur la cybercriminalité dans les cas où ces dernières sont insuffisantes. Elle reconnaît également la nécessité de promouvoir la coopération internationale dans la lutte contre la cybercriminalité et soutient une série de programmes de renforcement des capacités dans plusieurs pays à travers le monde, y compris des pays en développement¹³. La Commission soutient les travaux menés par le Groupe d'experts intergouvernemental sur le phénomène de la cybercriminalité que les Nations unies ont créé, par la Commission des Nations unies pour la prévention du crime et la justice pénale, par l'Office des Nations unies contre la drogue et le crime (ONUDC), par le Comité de la Convention de Budapest sur la cybercriminalité ainsi que par d'autres instances.

Les négociations relatives à la convention internationale devraient porter sur les règles communes de l'UE visant à lutter contre la cybercriminalité. Parmi ces règles pourraient figurer notamment la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie¹⁴, qui prévoit des mesures à l'égard de phénomènes nouveaux dans l'environnement en ligne comme le «grooming» ou pédopiégeage (qui consiste, pour les auteurs d'infractions, à se faire passer pour des enfants en vue d'attirer des mineurs à des fins d'abus sexuels); la directive 2013/40/UE relative aux attaques contre les systèmes d'information¹⁵, qui vise à contrer les cyberattaques à grande échelle en imposant aux États membres de renforcer leur arsenal législatif en matière de cybercriminalité et d'instaurer un niveau élevé de sanctions pénales; et la directive (UE) 2019/713 concernant la lutte contre la fraude et la contrefaçon des moyens de

¹⁰ [COM\(2020\) 605 final](#) du 27.7.2020.

¹¹ [COM\(2021\) 170 final](#) du 14.4.2021.

¹² [COM\(2021\) 799 final](#) du 8.12.2021.

¹³ Parmi ces programmes, on peut citer l'Action globale sur la cybercriminalité élargie (GLACY+) ainsi que les projets CyberEast et CyberSouth, cofinancés par l'UE et le Conseil de l'Europe et gérés par ce dernier.

¹⁴ Directive 2011/93/UE du 13.12.2011.

¹⁵ Directive 2013/40/UE du 12.8.2013.

paiement autres que les espèces¹⁶, qui harmonise les éléments constitutifs des agissements délictueux commis par des personnes physiques ou morales en ce qui concerne les moyens de paiement autres que les espèces et élargit la responsabilité pénale à l'utilisation frauduleuse des monnaies virtuelles et des porte-monnaie électroniques. D'autres instruments de l'UE prévoient des règles communes visant à lutter contre des infractions, telles que le terrorisme, la traite des êtres humains, le trafic de drogues, le trafic illicite d'armes, le blanchiment de capitaux, la corruption et la criminalité organisée, qui sont susceptibles d'être facilitées par le recours à des systèmes d'information.

Les négociations devraient également porter sur des mesures de procédure pénale et de coopération. Le cadre juridique actuel de l'UE comprend des instruments concernant la coopération des services répressifs et judiciaires en matière pénale, comme la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale¹⁷, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne¹⁸, le règlement (UE) 2018/1727 relatif à Eurojust¹⁹, le règlement (UE) 2016/794 relatif à Europol²⁰, le règlement (UE) 2017/1939 mettant en œuvre une coopération renforcée concernant la création du Parquet européen²¹, la décision-cadre 2002/465/JAI du Conseil relative aux équipes communes d'enquête²², 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 procédures pénales²³. Les propositions sur l'accès transfrontière aux preuves électroniques²⁴, présentées en avril 2018 par la Commission, et le train de mesures sur la coopération policière²⁵, actuellement examinés dans le cadre de la procédure législative de l'UE, sont également pertinents. Sur le plan extérieur, l'Union européenne a conclu plusieurs accords bilatéraux avec des pays tiers, comme les accords d'entraide judiciaire respectivement avec les États-Unis d'Amérique et le Japon²⁶.

L'Union a également adopté plusieurs directives qui renforcent les droits procéduraux des suspects et des personnes poursuivies²⁷. La protection des données à caractère personnel est un droit fondamental consacré à l'article 16 du TFUE et à l'article 8 de la charte des droits

¹⁶ Directive (UE) 2019/713 du 17.4.2019.

¹⁷ Directive 2014/41/UE du 3.4.2014.

¹⁸ Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne du 29.5.2020.

¹⁹ Règlement (UE) 2018/1727 du 14.11.2018.

²⁰ Règlement (UE) 2016/794 du 11.5.2016.

²¹ Règlement (UE) 2017/1939 du Conseil du 12.10.2017.

²² Décision-cadre 2002/465/JAI du Conseil du 13.6.2002.

²³ Décision-cadre 2009/948/JAI du Conseil du 30.11.2009.

²⁴ Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final, et proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM(2018) 226 final du 17.4.2018.

²⁵ Proposition de recommandation du Conseil relative à la coopération policière opérationnelle, COM(2021) 780, proposition de directive relative à l'échange d'informations entre les services répressifs des États membres, abrogeant la décision-cadre 2006/960/JAI du Conseil, COM(2021) 782, et proposition de règlement relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), COM(2021) 784, du 8.12.2021.

²⁶ Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire du 25.6.2003.

Accord entre l'Union européenne et le Japon relatif à l'entraide judiciaire en matière pénale (2009).

²⁷ Directive 2010/64/UE du 20.10.2010; directive 2012/13/UE du 22.5.2012; directive 2013/48/UE du 22.10.2013; directive (UE) 2016/1919 du 26.10.2016; directive (UE) 2016/800 du 11.5.2016; directive (UE) 2016/343 du 9.3.2016.

fondamentaux de l'Union européenne. Le traitement des données à caractère personnel doit être effectué conformément au règlement (UE) 2016/679 (le règlement général sur la protection des données)²⁸ et à la directive (UE) 2016/680 (la directive en matière de protection des données dans le domaine répressif)²⁹. Le droit fondamental des personnes au respect de leur vie privée et familiale, de leur domicile ainsi que de leurs communications est également consacré à l'article 7 de la charte des droits fondamentaux. Il comprend le respect de la confidentialité des communications ainsi que la protection de l'équipement terminal de l'utilisateur, en tant qu'éléments essentiels. Le traitement des données de communications électroniques doit être effectué conformément à la directive 2002/58/CE (la directive «vie privée et communications électroniques»)³⁰.

Lors des négociations, il conviendrait de faire en sorte que les dispositions d'une future convention des Nations unies offrent la protection des droits de l'homme la plus élevée possible et que les États membres soient en mesure de se conformer au droit de l'Union, compte tenu également de son évolution à venir.

- **Cohérence avec les autres politiques de l'Union**

L'Union européenne fait la promotion systématique de la convention de Budapest en tant que cadre juridique de référence utile et souple pour la coopération internationale dans la lutte contre la cybercriminalité. Elle soutient l'adhésion de pays tiers à cette convention, ce qui leur permet de mettre en place un cadre juridique national minimal pour combattre la cybercriminalité ainsi que de prévoir les moyens nécessaires pour les enquêtes et les poursuites, facilitant ainsi la coopération avec les autres parties à la convention³¹.

L'UE, représentée par la Commission, a également pris une part active aux négociations sur le deuxième protocole additionnel à la convention de Budapest³². Ce protocole sera ouvert à la signature en mai 2022. Étant donné que les matières faisant l'objet du deuxième protocole additionnel relèvent de la compétence exclusive de l'Union, la Commission a, le 25 novembre 2021, adopté deux propositions de décision du Conseil autorisant les États membres de l'UE à signer³³ et à ratifier³⁴, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité.

Dès lors, il faudra également veiller, lors des négociations, à la compatibilité et à la cohérence avec la convention de Budapest sur la cybercriminalité et avec ses protocoles additionnels.

²⁸ Règlement (UE) 2016/679 du 27.4.2016.

²⁹ Directive (UE) 2016/680 du 27.4.2016.

³⁰ Directive 2002/58/CE du 12.7.2002, modifiée par la directive 2009/136/CE du 25.11.2009.

³¹ Voir, par exemple, les conclusions du Conseil sur la cyberdiplomatie du 10 février 2015, document 6122/15.

³² Décision du Conseil autorisant la Commission européenne à participer, au nom de l'Union européenne, aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe, référence 9116/19.

³³ Proposition de décision du Conseil autorisant les États membres à signer, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, COM(2021) 718 final du 25.11.2021.

³⁴ Proposition de décision du Conseil autorisant les États membres à ratifier, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, COM(2021) 719 final du 25.11.2021.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

L'article 218, paragraphe 3, du traité sur le fonctionnement de l'Union européenne (TFUE) dispose que la Commission présente des recommandations au Conseil, qui adopte une décision autorisant l'ouverture de négociations et désignant le négociateur de l'Union. Conformément à l'article 218, paragraphe 4, du TFUE, le Conseil peut adresser des directives au négociateur.

- **Subsidiarité (en cas de compétence non exclusive)**

Une action unilatérale ne saurait constituer une alternative car elle ne procurerait pas une base suffisante pour la coopération avec les pays tiers. L'adhésion à un accord multilatéral tel qu'une éventuelle future convention des Nations unies, que l'Union aura pu négocier, est plus efficace que l'ouverture de négociations bilatérales avec différents pays tiers.

- **Proportionnalité**

La présente initiative ne va pas au-delà de ce qui est nécessaire pour atteindre les objectifs qui sont en jeu.

- **Choix de l'instrument**

Une recommandation, de la Commission, de décision du Conseil autorisant l'ouverture de négociations est conforme à l'article 218, paragraphe 3, du TFUE, en application duquel la Commission présente des recommandations au Conseil, qui adopte une décision autorisant l'ouverture de négociations.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

Sans objet.

- **Consultation des parties intéressées**

Le 14 janvier 2022, la Commission a publié sur son site web un appel à contributions concernant la présente initiative, qui est restée accessible pour commentaires pendant quatre semaines. Les (cinq) réponses individuelles à cet appel à contributions ont été publiées sur le site web consacré à la consultation. Les considérations ainsi formulées ont été prises en compte lors de l'élaboration de la présente proposition.

- **Obtention et utilisation d'expertise**

La Commission a tenu compte des avis exprimés par les experts des États membres durant les discussions menées au sein des groupes de travail compétents du Conseil lors de la préparation des négociations.

- **Analyse d'impact**

Sans objet.

- **Réglementation affûtée et simplification**

Sans objet.

- **Droits fondamentaux**

Les négociations porteront probablement sur des éléments susceptibles de constituer une atteinte aux droits fondamentaux, tels que des mesures de procédure pénale, la définition d'infractions pénales pouvant servir de fondement à des poursuites pénales ou l'accès aux données à caractère privé d'une personne obtenues dans le contexte d'une procédure pénale. Les dispositions devant être négociées pourraient porter atteinte, par exemple, au droit à accéder à un tribunal impartial, au droit au respect de la vie privée et au droit à la protection des données à caractère personnel. La participation aux négociations au nom de l'Union européenne devrait viser à préserver le niveau de protection des droits fondamentaux dans l'Union, de sorte qu'il est proposé, par la présente initiative, de rechercher un degré de protection élevé de ces droits.

4. INCIDENCE BUDGÉTAIRE

La proposition n'a pas d'incidence sur le budget de l'Union. Les États membres de l'UE pourraient devoir supporter des coûts ponctuels pour la mise en œuvre de la convention une fois les négociations achevées, mais il n'est pas possible de déterminer ces coûts à ce stade, étant donné que les négociations n'ont pas encore complètement commencé.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Le processus de négociation devrait durer jusqu'en 2024, après quoi la signature et la conclusion de la convention pourraient avoir lieu. L'initiative propose que soit suivi un processus de négociation ouvert, inclusif et transparent.

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

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 27 décembre 2019, l'Assemblée générale des Nations unies a adopté la résolution 74/247 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et a décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles³⁵. Il convient que l'Union participe aux négociations relatives à cette convention.
- (2) L'Union a adopté des règles communes qui coïncident avec plusieurs éléments envisagés pour cette convention. Ces règles communes consistent en un ensemble complet d'instruments relatifs au droit pénal matériel³⁶, à la coopération policière et judiciaire en matière pénale³⁷, aux normes minimales en matière de droits

³⁵ Résolution adoptée par l'Assemblée générale le 27 décembre 2019 sur la base du rapport de la Troisième Commission (A/74/401), Lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles, [A/RES/74/247](#).

³⁶ Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, [JO L 335 du 17.12.2011, p. 1](#); directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, [JO L 218 du 14.8.2013, p. 8](#); directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil, PE/89/2018/REV/3, [JO L 123 du 10.5.2019, p. 18](#).

³⁷ 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

procéduraux³⁸, et aux garanties en matière de protection des données et de la vie privée³⁹. Il conviendra de tenir également compte de futures règles communes⁴⁰.

- (3) Par conséquent, une nouvelle convention internationale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles est susceptible d'affecter des règles communes de l'Union ou d'en altérer la portée.
- (4) 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 relatives à une nouvelle convention internationale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

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 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, JO L 130 du 1.5.2014, p. 1.

³⁸ 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.

³⁹ 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; 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; 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.

⁴⁰ 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.

- (5) 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 et a rendu un avis le ...
- (6) [Conformément aux articles 1^{er} et 2 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption de la présente décision et n'est pas liée par celle-ci ni soumise à son application.]
- [OU]
- [Conformément aux articles 1^{er} et 2 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande a notifié [, par lettre du ... ,] son souhait de participer à l'adoption et à l'application de la présente décision.]
- (7) Conformément aux articles 1^{er} et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente décision et n'est pas lié par celle-ci ni soumis à son application,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La Commission est autorisée à négocier, au nom de l'Union, une convention générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

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 présente décision et son annexe sont publiées immédiatement après leur adoption.

Article 5

La Commission est destinataire de la présente décision.

Fait à Bruxelles, le

Par le Conseil
Le président