COM(2025) 415 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2024/2025

Reçu à la Présidence de l'Assemblée nationale
le 04 septembre 2025

Enregistré à la Présidence du Sénat
le 04 septembre 2025

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de décision du Conseil relative à la signature, au nom de l’Union européenne, de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d’information et de communication et pour la communication de preuves sous forme électronique d’infractions graves»

E 19923

Conseil de
l'Union européenne

Bruxelles, le 16 juillet 2025
(OR. en)

11553/25

Dossier interinstitutionnel:
2025/0230 (NLE)

CYBER 211
COPEN 210
JAI 1066
COPS 381
RELEX 998
JAIEX 78
TELECOM 243
POLMIL 209
CFSP/PESC 1145
ENFOPOL 268
DATAPROTECT 153

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	16 juillet 2025
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2025) 415 final
Objet:	Proposition de DÉCISION DU CONSEIL relative à la signature, au nom de l'Union européenne, de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves»

Les délégations trouveront ci-joint le document COM(2025) 415 final.

p.j.: COM(2025) 415 final

COMMISSION
EUROPÉENNE

Bruxelles, le 16.7.2025
COM(2025) 415 final

2025/0230 (NLE)

Proposition de

DÉCISION DU CONSEIL

relative à la signature, au nom de l'Union européenne, de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves»

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Objectifs de la proposition

La présente proposition vise à obtenir du Conseil de l'Union européenne (ci-après le «Conseil») l'autorisation, pour la Commission européenne (ci-après la «Commission»), de signer la convention des Nations unies contre la cybercriminalité (ci-après la «convention») au nom de l'Union européenne[1].

La Commission présentera également une proposition de décision du Conseil autorisant la Commission à conclure la convention au nom de l'Union européenne. Ensemble, ces propositions font suite à l'engagement pris par la Commission dans sa communication intitulée «ProtectEU: une stratégie européenne de sécurité intérieure»[2].

La menace que la cybercriminalité fait peser sur la sécurité des citoyens et des entreprises dans l'Union européenne (UE) s'aggrave[3]. D'après l'évaluation de la menace que représente la criminalité organisée sur l'internet réalisée par Europol, au cours des dix dernières années, les menaces liées à la cybercriminalité ont évolué de manière dynamique en termes de volume, d'intensité et de potentiel de préjudice[4]. Les cybercriminels exploitent des technologies émergentes, telles que l'intelligence artificielle (IA), afin d'automatiser leurs attaques, de pratiquer l'ingénierie sociale et de contourner les mesures de sécurité, ce qui rend les cyberattaques plus évolutives et plus efficientes. La récession économique, l'instabilité géopolitique et l'accroissement des inégalités mondiales renforcent les incitations à s'engager dans la cybercriminalité motivée par l'appât du gain[5]. L'ampleur et le nombre des infractions facilitées par les technologies de l'information et de la communication (TIC), telles que la fraude en ligne et les abus sexuels commis contre des enfants, continuent de croître. On estime que 1 030 milliards d'EUR ont été perdus dans le monde en 2024 en raison de la fraude en ligne[6]. Les signalements mondiaux d'abus sexuels commis contre des enfants sont passés de 1 million en 2010 à près de 36 millions en 2023, dont 1,3 million dans l'UE[7].

La cybercriminalité est un phénomène mondial et sans frontières et, depuis plus de dix ans, l'intensification de la coopération internationale dans la lutte contre ce phénomène constitue une priorité pour les pays du monde entier. En particulier, parce que l'internet ne connaît pas de frontières, les enquêtes en matière de cybercriminalité revêtent presque toujours un caractère transfrontière, ce qui nécessite une coopération étroite entre les autorités de

---

1 Le texte de la convention sera annexé à la proposition de décision du Conseil relative à la conclusion, au nom de l'Union européenne, de la convention.

2 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «ProtectEU: une stratégie européenne de sécurité intérieure», COM(2025) 148 final.

3 En 2023, les attaques par logiciel rançonneur, l'exploitation sexuelle des enfants et la fraude en ligne sont restées les manifestations les plus menaçantes de la cybercriminalité dans l'Union européenne (UE). Certains cybercriminels ciblant l'UE étaient établis au sein même de cette dernière, tandis que d'autres préféraient opérer depuis l'étranger, dissimulant leurs activités et leurs fonds illicites dans des pays tiers. Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2024.

4 Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2024.

5 Évaluation de la menace que représente la grande criminalité organisée (SOCTA) 2025.

6 Global State of Scams Report 2025 (rapport mondial 2025 sur l'état des escroqueries en ligne) (GASA).

7 Centre national américain pour les enfants disparus et exploités, https://www.missingkids.org/cybertiplinedata.

différents pays. Ces dernières années, le nombre de pays avec lesquels il est nécessaire de coopérer n'a cessé d'augmenter, étant donné que les cybercriminels se cachent sur des territoires propices dans le monde entier pour commettre leurs attaques contre l'UE et ses pays partenaires.

Les preuves électroniques revêtent une importance croissante pour les enquêtes pénales, concernant à la fois les infractions en ligne et les infractions traditionnelles, telles que le trafic de drogue, qui laissent souvent des traces en ligne, car les criminels planifient et coordonnent leurs activités en ligne et sur des applications. Ainsi, une enquête de la Commission a révélé que, dès 2018, les services répressifs et les autorités judiciaires avaient besoin d'avoir accès à des preuves électroniques dans au moins 85 % des enquêtes pénales, y compris en matière de cybercriminalité[8]. Les preuves d'infractions pénales sont de plus en plus détenues sous forme électronique par des fournisseurs de services situés dans des pays étrangers. Au moins 55 % des enquêtes comprennent une demande d'accès transfrontière à des preuves[9]. Afin de garantir l'efficacité de la justice pénale, il est nécessaire de prendre des mesures appropriées pour obtenir ces preuves de manière à défendre l'état de droit.

Par conséquent, des mesures visant à améliorer la communication des preuves électroniques dans le cadre d'enquêtes pénales sont prises aux niveaux national, de l'UE[10] et international.

La convention fait partie de ces mesures. Elle établit des règles communes au niveau mondial afin de renforcer la coopération en matière de cybercriminalité et la collecte de preuves sous forme électronique aux fins d'enquêtes ou de procédures pénales, créant ainsi une base pour la coopération avec de nombreux pays avec lesquels ni l'UE ni ses États membres n'ont conclu d'accord, tout en garantissant le respect de la législation et des valeurs de l'UE. Elle est compatible avec les instruments européens et internationaux existants et les complète.

Contexte

La convention du Conseil de l'Europe de 2001 sur la cybercriminalité (ci-après la «convention de Budapest»)[11] est le premier traité international sur la question. Elle facilite la lutte contre les infractions pénales commises au moyen des réseaux informatiques. La convention de Budapest est ouverte aux États membres du Conseil de l'Europe, ainsi que, sur invitation, aux pays tiers. À ce jour, elle compte 80 États parties, dont 26 États membres de l'Union européenne. Le deuxième protocole additionnel[12] à la convention de Budapest comprend des règles actualisées sur l'échange de preuves électroniques[13].

---

8 SWD(2018) 118 final.

9 SWD(2018) 118 final.

10 Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj) et directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

11 STCE nº 185.

12 STCE nº 224.

13 Le Conseil a adopté des décisions autorisant les États membres à signer et à ratifier le deuxième protocole additionnel dans l'intérêt de l'UE: décision (UE) 2022/722 du Conseil du 5 avril 2022 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 (JO L 134 du 11.5.2022, p. 15, ELI: http://data.europa.eu/eli/dec/2022/722/oj) et décision (UE) 2023/436 du Conseil du 14 février 2023

L'Union européenne et ses États membres sont également parties à deux des principaux instruments de justice pénale des Nations unies dont l'adoption est presque universelle, à savoir la convention des Nations unies contre la criminalité transnationale organisée (convention CTO)[14] et la convention des Nations unies contre la corruption (CNUCC)[15].

Les dispositions de la nouvelle convention sont alignées sur ces trois instruments internationaux établis et largement adoptés et compatibles avec ceux-ci.

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 (ci-après le «GIE») en vue de faire une étude approfondie du phénomène de la cybercriminalité.

L'Assemblée générale des Nations unies a adopté la résolution 73/187 du 17 décembre 2018 sur «la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles». Le 27 décembre 2019, l'Assemblée générale des Nations unies 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 (ci-après 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-ci.

---

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 (JO L 63 du 28.2.2023, p. 48, ELI: http://data.europa.eu/eli/dec/2023/436/oj).

[14] Doc. A/55/383. L'UE a signé la convention CTO le 12 décembre 2000 et l'a ratifiée le 21 mai 2004; elle a également ratifié ses protocoles sur le trafic de migrants et la traite des êtres humains. Voir 2004/579/CE: décision du Conseil du 29 avril 2004 relative à la conclusion, au nom de la Communauté européenne, de la convention des Nations unies contre la criminalité transnationale organisée (JO L 261 du 6.8.2004, p. 69, ELI: http://data.europa.eu/eli/dec/2004/579/oj), 2006/616/CE: décision du Conseil du 24 juillet 2006 relative à la conclusion, au nom de la Communauté européenne, du protocole contre le trafic illicite de migrants par terre, air et mer, additionnel à la convention des Nations unies contre la criminalité transnationale organisée en ce qui concerne les dispositions du protocole, dans la mesure où celles-ci relèvent des articles 179 et 181 A du traité instituant la Communauté européenne (JO L 262 du 22.9.2006, p. 24, ELI: http://data.europa.eu/eli/dec/2006/616/oj) et 2006/619/CE: décision du Conseil du 24 juillet 2006 relative à la conclusion, au nom de la Communauté européenne, du protocole additionnel à la convention des Nations unies contre la criminalité transnationale organisée visant à prévenir, à réprimer et à punir la traite des personnes, en particulier des femmes et des enfants, en ce qui concerne les dispositions du protocole dans la mesure où celles-ci relèvent de la troisième partie, titre IV, du traité instituant la Communauté européenne (JO L 262 du 22.9.2006, p. 51, ELI: http://data.europa.eu/eli/dec/2006/619/oj).

[15] Nations unies, Recueil des traités, vol. 2349, p. 41, doc. A/58/422. L'UE a signé la CNUCC le 15 septembre 2005 et l'a ratifiée le 12 novembre 2008. Voir 2008/801/CE: décision du Conseil du 25 septembre 2008 relative à la conclusion, au nom de la Communauté européenne, de la convention des Nations unies contre la corruption (JO L 287 du 29.10.2008, p. 1, ELI: http://data.europa.eu/eli/dec/2008/801/oj).

Le 24 mai 2022, le Conseil a autorisé la Commission à participer, au nom de l'Union européenne, aux négociations relatives à la convention[16]. La Commission y a participé conformément à la décision du Conseil, en s'inspirant des directives de négociation qui y sont énoncées. La Commission a reçu le soutien du Service européen pour l'action extérieure (SEAE). Elle a systématiquement consulté le comité spécial du Conseil pour les négociations au sujet de la position de l'Union et a veillé à la compatibilité de la convention avec l'acquis pertinent de l'UE.

Conformément à l'accord-cadre sur les relations entre le Parlement européen et la Commission européenne[17], la Commission a également tenu le Parlement européen informé des négociations.

La Commission a également informé le Contrôleur européen de la protection des données (CEPD) et le comité européen de la protection des données pendant les négociations et après leur conclusion.

Le comité spécial s'est réuni huit fois en sessions formelles entre le 28 février 2022 et le 9 août 2024. Il a également tenu des sessions informelles entre les sessions formelles et cinq sessions intersessions afin de consulter un large éventail de parties prenantes, notamment des organisations intergouvernementales mondiales et régionales, des organisations non gouvernementales, des organisations de la société civile, des établissements universitaires et le secteur privé.

Le 8 août 2024, le comité spécial a approuvé par consensus le projet de texte de la convention et le projet de résolution de l'Assemblée générale des Nations unies l'accompagnant. L'Assemblée générale des Nations unies a adopté ces deux documents par consensus le 24 décembre 2024[18]. La convention devrait être ouverte à la signature à Hanoï (Viêt Nam) le 25 octobre 2025, puis au siège de l'Organisation des Nations unies à New York jusqu'au 31 décembre 2026.

La convention entrera en vigueur après que 40 États parties auront exprimé leur consentement à être liés par elle, conformément aux dispositions de son article 65, paragraphes 1 et 2.

Conformément à une pratique bien établie en ce qui concerne la convention CTO et la CNUCC, la convention prévoit qu'une organisation régionale d'intégration économique, telle que l'Union européenne, peut signer et ratifier la convention si au moins un de ses États membres la signe et la ratifie.

Justification de la proposition

La convention est conforme aux objectifs de l'Union énoncés dans ProtectEU, la stratégie européenne de sécurité intérieure de 2025, visant à lutter contre la criminalité et à faciliter l'accès aux preuves numériques pour toutes les infractions au moyen d'instruments internationaux, tels que la convention. Elle complète les instruments européens et internationaux existants auxquels l'UE et/ou ses États membres sont parties, tels que la convention de Budapest du Conseil de l'Europe, et contribue ainsi à la lutte de l'UE contre la criminalité transnationale.

---

16 Décision (UE) 2022/895 du Conseil du 24 mai 2022 autorisant l'ouverture de négociations, au nom de l'Union européenne, 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 (JO L 155 du 8.6.2022, p. 42, ELI: http://data.europa.eu/eli/dec/2022/895/oj).

17 Référence L 304/47.

18 Résolution adoptée par l'Assemblée générale des Nations unies le 24 décembre 2024, doc. A/RES/79/243.

Premièrement, en tant qu'instrument des Nations unies, la convention a une portée plus large en termes d'adhésion que les instruments européens et internationaux existants. À cet égard, elle s'apparente à de précédents instruments des Nations unies relatifs à la coopération en matière pénale dont l'adoption est presque universelle, tels que la convention CTO et la CNUCC. Elle peut ainsi permettre de renforcer la coopération contre la cybercriminalité à l'échelle mondiale.

Deuxièmement, la convention s'inspire des dispositions de la convention de Budapest en matière d'incrimination et est donc susceptible de renforcer encore la coopération sur la base d'un cadre juridique établi de longue date et éprouvé. Compte tenu de son adoption plus récente, la convention introduit également de nouvelles dispositions en matière d'incrimination relatives à des infractions qui ont connu une augmentation spectaculaire au cours des dernières années: la fraude en ligne, la sollicitation ou manipulation psychologique aux fins de commettre une infraction sexuelle à l'encontre d'un enfant, et la diffusion non consentie d'images intimes. Ces actes sont déjà érigés en infraction pénale au niveau de l'UE, mais pas encore à l'échelle mondiale.

Troisièmement, la convention permet l'échange de preuves électroniques entre les autorités de ses États parties sur des formes graves de criminalité également en hausse, notamment les infractions liées au terrorisme et à la criminalité transnationale organisée. Cette limitation aux infractions graves restreint le recours au mécanisme aux seuls cas graves, ce qui contribue à garantir la proportionnalité. Elle évite également de surcharger les autorités nationales de demandes et reflète les différents niveaux de confiance dans la coopération qui existent au niveau international.

Quatrièmement, la convention complète les instruments internationaux existants, tels que la convention de Budapest, en incluant des mesures procédurales relatives à la protection des victimes et des témoins, des outils de recouvrement du produit de la cybercriminalité ainsi que des mesures de coopération internationale en ce qui concerne le transfèrement des personnes condamnées et le transfert des procédures pénales, les enquêtes conjointes et la coopération en matière répressive.

Cinquièmement, la convention comprend un chapitre sur l'assistance technique et le renforcement des capacités afin d'aider les pays en développement à renforcer leurs capacités et de leur permettre de contribuer à la lutte mondiale contre la cybercriminalité.

Sixièmement, la convention impose à ses États parties de respecter les droits de l'homme, y compris les droits et garanties procéduraux en matière pénale (tels que le droit à un procès équitable, les droits de la défense, le contrôle juridictionnel ou une autre forme de contrôle indépendant), ainsi que le droit à la protection des données à caractère personnel, pour chaque mesure qu'elle prévoit. Compte tenu de sa vocation universelle et des différences qui existent dans le niveau de protection des droits de l'homme à travers le monde, la convention comprend des dispositions visant à exclure son utilisation à des fins de violation des droits de l'homme et à fournir aux États parties des motifs sans précédent pour refuser de coopérer avec d'autres parties dans de tels cas. De plus amples informations à cet égard sont fournies dans les sections «*Cohérence avec les dispositions existantes dans le domaine d'action*», «*Droits fondamentaux*» et «*Explication détaillée de certaines dispositions de la proposition*» ci-dessous. Ces dispositions font de la convention le premier instrument de ce type à offrir une protection et des garanties aussi complètes en matière de droits de l'homme. Dès son entrée en vigueur, la convention deviendra une référence pour les futurs instruments internationaux et contribuera à intégrer ces garanties concernant les droits de l'homme dans la coopération mondiale en matière pénale.

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

La lutte contre la cybercriminalité est une priorité pour l'Union européenne, comme l'ont indiqué le Conseil dans ses orientations stratégiques de la programmation législative et opérationnelle dans l'espace de liberté, de sécurité et de justice de 2024[19] et la Commission dans sa communication de 2025 intitulée «ProtectEU: une stratégie européenne de sécurité intérieure», qui annonce des mesures de l'UE pour lutter contre la criminalité en ligne et faciliter l'accès aux preuves numériques pour toutes les infractions, passant notamment par des instruments internationaux d'échange d'informations et de preuves, y compris la signature et la conclusion en temps utile de la convention.

La Commission est consciente de 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 les législations nationales sur la cybercriminalité dans les cas où ces dernières sont insuffisantes. Elle est également consciente de 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 développement[20]. La Commission soutient les travaux menés par le GIE, la Commission des Nations unies pour la prévention du crime et la justice pénale, l'Office des Nations unies contre la drogue et le crime (ONUDC), le comité de la convention de Budapest sur la cybercriminalité et d'autres organes.

Les dispositions de la convention sont conformes aux règles et politiques de l'UE dans les domaines de la coopération judiciaire en matière pénale, de la coopération policière et de la protection des données, ainsi qu'aux accords bilatéraux et multilatéraux pertinents auxquels l'Union européenne est déjà partie.

Réserves et notifications

La convention ne contient pas de disposition spécifiquement consacrée aux réserves. Toutefois, elle prévoit explicitement des réserves dans certaines de ses dispositions [article 11, paragraphe 3, article 23, paragraphe 3, alinéa a), article 23, paragraphe 3, partie conclusive, article 42, paragraphe 5, article 63, paragraphes 3 et 4] et autorise implicitement d'autres réserves pour autant que celles-ci soient conformes à l'article 19, alinéa c), de la convention de Vienne sur le droit des traités[21] et au droit international coutumier et ne soient donc pas incompatibles avec l'objet et le but de la convention. Par conséquent, la convention accorde une grande souplesse en ce qui concerne les réserves. Les États membres devraient adopter une approche uniforme en matière de réserves et de notifications, conformément à l'annexe I de la présente décision. Les réserves et les notifications devraient être compatibles avec le droit de l'Union et le droit international public et ne pas porter atteinte à l'objet et au but de la convention. Les conditions et garanties en matière de droits de l'homme reconnues et prévues par la convention font partie de son objet et de son but et ne peuvent donc pas donner lieu à des réserves.

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

La convention est cohérente avec les règles et politiques pertinentes de l'Union européenne dans les domaines qu'elle couvrira (coopération internationale et entraide judiciaire entre les

[19] Orientations stratégiques de la programmation législative et opérationnelle dans l'espace de liberté, de sécurité et de justice, 28 novembre 2024, point 19.

[20] Voir, par exemple, l'action globale renforcée sur la cybercriminalité (GLACY-e), https://www.coe.int/en/web/cybercrime/glacy-e.

[21] Nations unies, Recueil des traités, vol. 1155, p. 331.

autorités publiques des États membres et entre les États membres et les pays tiers, comme décrit à la section «*Cohérence avec les dispositions existantes dans le domaine d'action*») et avec les accords bilatéraux et multilatéraux pertinents auxquels l'Union européenne est déjà partie. Elle n'a pas d'incidence sur d'autres domaines d'action de l'Union.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La proposition est présentée en vertu l'article 218, paragraphe 5, du traité sur le fonctionnement de l'Union européenne (TFUE). L'article 218 du TFUE établit la procédure de négociation et de conclusion d'accords entre l'Union européenne et des pays tiers ou des organisations internationales. Son paragraphe 5 prévoit en particulier que le Conseil, sur proposition de la Commission en tant que négociateur, adopte une décision autorisant la signature d'un accord au nom de l'Union européenne.

La base juridique matérielle d'une décision au titre de l'article 218, paragraphe 5, du TFUE dépend avant tout de l'objectif et du contenu de l'accord international envisagé pour lequel une position est prise au nom de l'Union. Si l'accord international envisagé poursuit deux finalités ou comporte deux composantes et si l'une de ces finalités ou composantes est identifiable comme étant la principale, tandis que l'autre n'est qu'accessoire, la décision au titre de l'article 218, paragraphe 5, du TFUE doit être fondée sur une seule base juridique matérielle, à savoir celle exigée par la finalité ou la composante principale ou prédominante.

Si l'accord international envisagé poursuit simultanément plusieurs finalités ou comporte plusieurs composantes qui sont liées de façon indissociable, sans que l'une soit accessoire par rapport à l'autre, la base juridique matérielle d'une décision au titre de l'article 218, paragraphe 5, du TFUE devra comporter, à titre exceptionnel, les diverses bases juridiques correspondantes.

En ce qui concerne les questions touchant à la facilitation de la coopération entre les autorités judiciaires ou équivalentes dans le cadre des procédures pénales et de l'exécution des décisions, la base juridique matérielle est l'article 82, paragraphe 1, du TFUE. En ce qui concerne la définition des infractions pénales dans le domaine de la cybercriminalité, la base juridique matérielle est l'article 83, paragraphe 1, du TFUE. En ce qui concerne les mesures relatives à la coopération des services répressifs, la base juridique matérielle est l'article 87, paragraphe 2, du TFUE. En ce qui concerne la protection des données à caractère personnel, la base juridique matérielle est l'article 16 du TFUE.

• Compétence de l'Union

La convention vise à lutter contre la cybercriminalité, notamment en érigeant en infraction pénale certains types graves d'actes préjudiciables et en instaurant une coopération internationale à cette fin, y compris en ce qui concerne les preuves électroniques. Ces questions relèvent d'une compétence partagée entre l'Union et les États membres, conformément à l'article 4, paragraphe 2, point j), du TFUE.

Certaines dispositions de la convention, notamment la disposition relative à la protection des données, relèvent de domaines couverts dans une large mesure par des règles communes susceptibles d'être affectées ou dont le champ d'application pourrait être modifié par la convention. Par conséquent, en ce qui concerne ces domaines et conformément à l'article 3, paragraphe 2, du TFUE, l'Union dispose d'une compétence externe exclusive pour la signature de la convention.

La signature de la convention par la Commission européenne, dans l'intérêt de l'Union, peut donc avoir lieu sur la base de l'article 16, de l'article 82, paragraphe 1, de l'article 83, paragraphe 1, de l'article 87, paragraphe 1 et de l'article 218, paragraphe 5, du TFUE.

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

L'action au niveau de l'UE vise à promouvoir une application harmonieuse des dispositions de la convention dans les États membres de l'UE et garantit sa compatibilité avec les instruments existants et futurs de l'UE. En outre, l'action de l'UE dans ce domaine renforce le poids et l'influence combinés de l'UE et de ses États membres concernant les mécanismes de mise en œuvre de la convention, tels que sa conférence des États parties (article 57), ainsi que la négociation future de protocoles (article 62) à celle-ci.

- **Proportionnalité**

En ce qui concerne la présente proposition, les objectifs de l'Union, tels qu'ils sont énoncés dans la section «*Justification de la proposition*» ci-dessus, ne peuvent être atteints que par la conclusion d'un accord international contraignant prévoyant les mesures de coopération nécessaires tout en garantissant une protection appropriée des droits fondamentaux. La convention atteint cet objectif. Les dispositions de la convention sont limitées à ce qui est nécessaire pour atteindre ses principaux objectifs et n'empiètent pas sur les instruments existants de l'UE ou sur les instruments internationaux auxquels l'UE est partie.

- **Choix de l'instrument**

L'article 218, paragraphe 5, du TFUE prévoit que la Commission ou le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, en fonction de l'objet de l'accord envisagé, soumet des propositions au Conseil, qui adopte une décision autorisant la signature d'un accord international. Compte tenu de l'objet de la convention, il convient que la Commission présente une proposition en ce sens.

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 resté ouvert pour commentaires pendant quatre semaines. Les 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 considération lors de l'élaboration de la proposition de la Commission relative à l'ouverture de négociations sur la convention.

Afin de garantir une plus grande transparence du processus, la résolution 75/282 de l'Assemblée générale des Nations unies, définissant les questions d'organisation concernant le comité spécial, a prévu que des représentants des organisations intergouvernementales mondiales et régionales compétentes, y compris des représentants d'organismes, d'institutions spécialisées et de fonds des Nations unies, ainsi que des représentants de commissions techniques du Conseil économique et social, participeraient en tant qu'observateurs aux sessions de fond dudit comité. En outre, cette résolution a permis aux organisations non gouvernementales (y compris les organisations intergouvernementales mondiales et régionales, les organisations non gouvernementales, les organisations de la société civile, les

établissements universitaires et le secteur privé) de s'inscrire et de participer aux sessions du comité spécial, où elles ont régulièrement eu la possibilité de présenter leur point de vue sur les chapitres examinés lors des sessions plénières. Conformément à cette résolution, cinq sessions de consultation intersessions ont été organisées avec les parties prenantes. Ces dernières ont également pu soumettre des contributions écrites, qui ont été publiées sur le site web du comité spécial.

La Commission, en sa qualité de négociateur, a également dialogué régulièrement avec diverses parties prenantes tout au long des négociations et tenu compte de leurs contributions.

- **Obtention et utilisation d'expertise**

Au cours des négociations, la Commission, en tant que représentante de l'Union, a consulté le comité spécial du Conseil pour les négociations, conformément à la décision du Conseil du 22 mai 2022 autorisant la Commission à participer, au nom de l'Union, aux négociations. En tant que membres de l'Organisation des Nations unies, les États membres de l'UE ont pu assister à toutes les sessions de négociation. La Commission a consulté leurs représentants sur la formulation de la position de l'Union tout au long des négociations. La Commission a également consulté régulièrement les parties prenantes (voir la section «*Consultations des parties intéressées*» ci-dessus).

- **Analyse d'impact**

Les incidences qui revêtent un intérêt sont présentées dans le présent exposé des motifs.

- **Réglementation affûtée et simplification**

La convention peut avoir des implications pour certaines autorités publiques et certaines catégories de fournisseurs de services. En raison d'une coopération internationale accrue en matière de partage de preuves électroniques pour lutter contre la cybercriminalité et les infractions facilitées par les TIC, le nombre de demandes de preuves électroniques que les autorités centrales des États membres de l'UE chargées de l'entraide judiciaire pourraient recevoir de leurs homologues d'autres États parties à la convention et ensuite transmettre, sous réserve de toutes les règles et procédures nationales applicables, aux fournisseurs de services établis dans leur État pourrait augmenter. Dans le même temps, le cadre juridique de la coopération internationale en matière de cybercriminalité que la convention établit à l'échelle mondiale, ainsi que les garanties et les conditions qu'elle contient, offriront aux fournisseurs de services une plus grande sécurité juridique en ce qui concerne les demandes d'accès aux données susceptibles de leur parvenir dans le cadre de la coopération entre États en matière pénale.

- **Droits fondamentaux**

La convention contient des garanties permettant aux États membres de l'UE de se conformer aux obligations en matière de droits de l'homme prévues par le droit international, le droit de l'Union et le droit national. Ces garanties empêchent également les États parties d'utiliser cet instrument des Nations Unies de manière abusive pour commettre ou légitimer des violations des droits de l'homme.

Les dispositions de la convention portent sur des mesures procédurales et de coopération internationale en matière pénale, telles que l'extradition, l'entraide judiciaire et l'échange de preuves électroniques, qui pourraient porter atteinte aux droits fondamentaux, tels que les droits à la liberté et à la protection contre les traitements inhumains et dégradants, ainsi que les droits au respect de la vie privée et à la protection des données à caractère personnel. La convention suit une approche fondée sur les droits et prévoit des conditions et des garanties solides en matière de droits de l'homme, tant horizontales que spécifiques au contexte, qui

sont conformes aux instruments internationaux existants concernant les droits de l'homme et la coopération en matière pénale. La convention tient également compte des risques en matière de droits de l'homme inhérents à la lutte contre la cybercriminalité et à la nature de l'internet. En ce qui concerne les obligations de ses États parties en matière de droits de l'homme, la convention fait à plusieurs reprises référence au «droit international des droits de l'homme». Cette expression large englobe à la fois les instruments internationaux et le droit international coutumier en matière de droits de l'homme et garantit ainsi l'application la plus large possible des obligations internationales dans ce domaine à toutes les futures parties à la convention, indépendamment de leur adhésion à des instruments internationaux spécifiques en matière de droits de l'homme.

L'article 6 prévoit une obligation générale pour les États parties de respecter les obligations que leur impose le droit international des droits de l'homme lors de la mise en œuvre de la convention. Il interdit également à toute partie à la convention d'interpréter cette dernière en ce sens qu'elle lui permettrait d'utiliser cet instrument juridique pour réprimer les droits de l'homme ou les libertés fondamentales. Afin de souligner cette obligation dans le contexte numérique dans lequel s'inscrit la convention, l'article 6, paragraphe 2, comprend également une liste non exhaustive des droits de l'homme et des libertés fondamentales qui sont plus susceptibles d'être touchés par d'éventuels abus dans le domaine numérique, y compris la liberté d'expression, de conscience, d'opinion, de religion ou de conviction, de réunion pacifique et d'association. En raison de son emplacement et de sa nature, cette disposition horizontale s'applique à l'ensemble de la convention et fait partie de l'objet et du but de cette dernière.

L'article 21, paragraphe 4, constitue également une disposition horizontale, relative à l'harmonisation des poursuites judiciaires, des jugements et des sanctions applicables aux infractions visées par la convention. Il impose aux États parties de veiller à ce que toute personne poursuivie pour une infraction établie conformément à la convention bénéficie de tous les droits et garanties prévus par le droit interne, dans le respect des obligations internationales applicables qui leur incombent, y compris le droit à un procès équitable et les droits de la défense.

L'article 24 établit également des conditions et des garanties horizontales, concernant les pouvoirs et les mesures procédurales prévus par la convention, tant au niveau interne qu'au niveau international. Il impose aux États parties de veiller à ce que, lors de l'exercice de leurs pouvoirs procéduraux, ceux-ci soient soumis à des conditions et garanties qui assurent la protection des droits de l'homme, conformément aux obligations qui leur incombent en vertu du droit international des droits de l'homme, et qui intègrent le principe de proportionnalité. Ces conditions et garanties applicables aux pouvoirs et procédures prévus par la convention incluent, entre autres, un contrôle juridictionnel ou une autre forme de contrôle indépendant, le droit à un recours efficace (qui englobe plusieurs mesures pour les personnes dont les droits de l'homme ont été violés), des motifs justifiant l'application, et la limitation du champ d'application et de la durée des pouvoirs et des procédures.

L'article 36 établit, pour la première fois dans un instrument de justice pénale des Nations unies, une disposition consacrée à la protection des données à caractère personnel. Il s'applique à tout transfert de données à caractère personnel effectué en vertu de la convention. Ces transferts ne peuvent avoir lieu que conformément au droit interne et aux obligations de droit international de l'État partie qui procède au transfert. Les États parties peuvent refuser de transférer des données à caractère personnel à un autre État partie si celles-ci ne peuvent pas être fournies conformément à leurs lois applicables concernant la protection des données. Afin d'assurer la conformité avec sa législation nationale en matière de protection des données à caractère personnel et d'être en mesure de donner suite à une demande de

coopération internationale, un État partie peut imposer des conditions appropriées à l'État requérant. Les États parties sont tenus de veiller à ce que leurs cadres juridiques respectifs prévoient l'application de garanties effectives et appropriées aux données à caractère personnel qu'ils reçoivent en vertu de la convention, que ce soit dans le cadre d'une demande de coopération internationale ou en réponse à une demande. Les États parties ne peuvent transférer les données à caractère personnel reçues à un pays tiers ou à une organisation internationale qu'avec l'autorisation préalable de l'État partie ayant procédé au transfert initial, lequel peut exiger que ladite autorisation soit fournie par écrit.

La convention prévoit de vastes garanties en matière d'extradition et d'entraide judiciaire. Les États parties ont la possibilité de refuser des demandes d'extradition ou d'entraide judiciaire en l'absence de double incrimination (article 37, paragraphe 1, et article 40, paragraphe 8).

La convention contient d'autres motifs de refus de coopération, qui sont conformes aux instruments internationaux existants. L'article 37, paragraphes 8 et 15, et l'article 40, paragraphes 8, 21 et 22, permettent aux États parties de refuser les demandes de coopération internationale dans un large éventail de cas, par exemple si la demande d'entraide judiciaire n'est pas faite conformément aux dispositions de l'article 40; si l'État partie requis estime que l'exécution de la demande est susceptible de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels (qui sont souvent interprétés au niveau international comme incluant également les considérations relatives aux droits de l'homme); dans le cas où le droit interne de l'État partie requis interdirait à ses autorités de prendre les mesures demandées face à une infraction analogue; dans le cas où cela serait contraire au système juridique de l'État partie requis concernant l'entraide judiciaire; et si l'État partie requis a de sérieuses raisons de penser que la demande a été présentée aux fins de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politiques, ou que donner suite à cette demande causerait un préjudice à cette personne pour l'une quelconque de ces raisons. L'application de cette dernière garantie aux mesures d'entraide judiciaire, telles que l'échange de preuves électroniques, est rare dans la plupart des instruments internationaux relatifs à la coopération en matière pénale. Elle constitue une garantie supplémentaire importante pour empêcher que des personnes, des organisations du secteur privé, des médias ou des organisations de la société civile et leurs biens ne soient pris pour cible. Cette garantie, les autres motifs de refus et l'exigence de double incrimination permettent aux États parties de refuser la coopération internationale dans les affaires qu'ils jugent motivées par des considérations politiques.

Les conditions et garanties relatives aux droits de l'homme reconnues et prévues par la convention font partie de son objet et de son but et sont indissociables des pouvoirs et procédures qu'elle prévoit. Dès lors, ces conditions et garanties ne peuvent pas faire l'objet de réserves.

La convention prévoit également un mécanisme d'examen périodique de sa mise en œuvre par sa conférence des États parties [article 57, paragraphe 5, alinéa f)]. Cet examen devrait porter sur toutes les dispositions de la convention, y compris ses conditions et garanties, conformément aux autres instruments et mécanismes internationaux existants dans le même domaine.

4. INCIDENCE BUDGÉTAIRE

La proposition n'a pas d'incidence sur le budget de l'Union. La mise en œuvre de la convention pourrait engendrer des coûts ponctuels pour les États membres de l'UE et leurs

autorités pourraient voir leurs coûts augmenter de manière modérée en raison de l'augmentation attendue du nombre de demandes de coopération internationale.

5. AUTRES ÉLÉMENTS

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

Les États membres étant tenus de mettre en œuvre la convention après sa signature et sa ratification, il n'existe pas de plan de mise en œuvre.

En ce qui concerne le suivi, la Commission participera aux réunions de la conférence des États parties, au cours desquelles l'Union européenne sera considérée comme une partie à la convention et pourra exercer son droit de vote en disposant d'un nombre de voix égal au nombre d'États membres parties à la convention en ce qui concerne l'adoption d'amendements et de protocoles additionnels à la convention. La Commission informera régulièrement le Parlement européen des résultats de l'examen et du suivi de la mise en œuvre de la convention menés par la conférence des États parties.

• Explication détaillée de certaines dispositions de la proposition

L'objectif de la convention est de renforcer la coopération internationale en ce qui concerne les infractions pénales établies dans la convention et la collecte de preuves électroniques relatives aux infractions définies dans la convention et à d'autres infractions graves aux fins d'enquêtes ou de procédures pénales spécifiques. À cet égard, la convention vise également à promouvoir l'assistance technique et le renforcement des capacités, notamment au profit des pays en développement.

Dispositions générales [chapitre premier (articles 1er à 6)]

Le chapitre premier définit le champ d'application général et l'objet de la convention ainsi que les termes qui y sont utilisés. Pour l'essentiel, ces dispositions sont des formulations standard inspirées de la convention de Budapest et des deux instruments existants des Nations unies en matière de justice pénale (convention CTO et CNUCC).

L'article 2 établit des définitions qui cadrent avec celles de la convention de Budapest, de son deuxième protocole additionnel et des deux instruments existants des Nations unies en matière de justice pénale (convention CTO et CNUCC). Par rapport à ces instruments, la convention contient une seule nouvelle définition, concernant les «données de contenu», qui s'inspire de la loi type de l'ONUDC sur l'entraide judiciaire en matière pénale[22] et de la définition figurant dans le règlement sur les preuves électroniques[23].

L'article 3 définit le champ d'application de la convention comme englobant la prévention des infractions pénales établies conformément à la convention, les enquêtes et les poursuites les concernant, ainsi que le recouvrement du produit de ces infractions. Le champ d'application de la convention s'étend également à la collecte et à la communication de preuves électroniques dans le cadre d'enquêtes ou de procédures pénales spécifiques en vertu des articles 23 et 35 [pour plus de détails, voir les sections «*Mesures procédurales et détection et*

---

22 Loi type de l'ONUDC sur l'entraide judiciaire en matière pénale (2007), telle que modifiée par les dispositions relatives aux preuves électroniques et à l'utilisation de techniques d'enquête spéciales (2022), E/CN.15/2022/CRP.6.

23 Voir le règlement (UE) 2023/1543 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, article 3, point 12).

répression [chapitre IV (articles 23 à 34)]» et «*Coopération internationale [chapitre V (articles 35 à 52)]*» ci-dessous].

L'article 4 prévoit que les infractions qui sont établies conformément à d'autres conventions et protocoles applicables des Nations unies (et auxquels les États parties sont parties) devraient être passibles de sanctions, qu'elles aient été commises hors ligne ou en ligne. Le deuxième paragraphe restreint le champ d'application de cet article, en soulignant que cette disposition ne constitue pas une base juridique permettant de créer des infractions nouvelles ou supplémentaires au-delà de celles prévues dans les conventions et protocoles applicables des Nations unies.

L'article 5 est une disposition standard relative au respect du principe de souveraineté, qui reprend les termes des dispositions correspondantes de la convention CTO et de la CNUCC.

L'article 6 constitue une disposition sans précédent par rapport aux deux instruments de justice pénale des Nations unies et à la convention de Budapest. Il délimite clairement l'objet et le but de la convention et constitue une garantie importante contre son utilisation inappropriée. Le paragraphe 1 prévoit, en tant qu'objectif général de haut niveau, que toutes les mesures prises pour mettre en œuvre la convention doivent être guidées par les obligations internationales en matière de droits de l'homme contractées par chaque État partie. Le paragraphe 2 complète cet objectif en réaffirmant que la convention ne doit pas être interprétée dans le but de violer des droits de l'homme, qu'ils soient économiques, sociaux, culturels ou civils et politiques. Cette disposition comprend une liste non exhaustive de droits considérés comme particulièrement exposés à des violations dans le cadre des mesures visant à lutter contre la cybercriminalité, tels que la liberté d'expression, de conscience, d'opinion, de religion ou de conviction, de réunion pacifique et d'association. Par conséquent, le champ d'application de la convention est également limité par cette disposition, qui empêche les États parties de tenter à l'avenir d'appliquer trop largement les mesures de coopération internationale prévues par la convention.

Incrimination [chapitre II (articles 7 à 21)]

Les articles 7 à 17 prévoient l'harmonisation de l'incrimination des actes et des éléments constitutifs d'infractions purement informatiques et de certaines infractions facilitées par les TIC. Les infractions purement informatiques (articles 7 à 11) s'inspirent des infractions énoncées dans la convention de Budapest. Les infractions facilitées par les TIC (articles 12 à 16) s'inspirent également de la convention de Budapest et les articles en question harmonisent, entre autres, l'infraction de fraude en rapport avec les systèmes d'information et de communication (y compris les escroqueries en tant que type de fraude), les infractions relatives à des contenus en ligne présentant des abus sexuels sur enfant, ainsi que les infractions de sollicitation aux fins de commettre une infraction sexuelle à l'encontre d'un enfant et la diffusion non consentie d'images intimes. Toutes les infractions visées dans la convention requièrent deux éléments essentiels: l'intention et le fait que l'infraction soit commise sans droit. Ce dernier élément est une exigence spécifique au contexte en matière de responsabilité pénale qui permet aux États parties de faire preuve de souplesse dans l'application, conformément à leur droit interne et à leurs obligations internationales. À cet égard, la condition voulant que l'infraction soit commise «sans droit» vise à garantir que, par exemple, les actes accomplis par des autorités répressives dans le cadre d'enquêtes sur des infractions ou les actes accomplis à des fins de sécurité, scientifiques, médicales, artistiques ou à d'autres fins légitimes, justifiées ou autorisées sont exclus du champ d'application de l'incrimination. À cet égard, l'article 14, paragraphe 4, prévoit une exemption explicite de l'incrimination pour les actes commis par des enfants en cas de contenus autoproduits les représentant et pour la production, la transmission ou la détention consenties de contenu décrit

à l'article 14, paragraphe 2, alinéas a) à c), lorsque les actes représentés sont légaux selon le droit interne et que ce contenu est réservé exclusivement à l'usage privé et consenti des personnes prenant part aux actes en question.

L'article 17 impose d'ériger en infraction pénale le blanchiment du produit du crime et s'inspire des dispositions correspondantes de la convention CTO et de la CNUCC. Selon les notes interprétatives sur certains articles de la convention, qui sont annexées à la résolution portant adoption de la convention, un acte n'est considéré comme une infraction au sens de l'article 17 que lorsque le comportement délictueux sous-jacent associé à l'infraction plus complexe de blanchiment du produit du crime est une infraction établie conformément aux articles 7 à 16 de la convention.

L'article 18 reproduit les dispositions correspondantes de la convention CTO et de la CNUCC concernant l'établissement de règles minimales en matière de responsabilité des personnes morales pour les infractions établies conformément à la convention (à savoir les infractions visées aux articles 7 à 17). Cette responsabilité est liée à la participation des personnes morales à l'une des infractions pénales codifiées aux articles 7 à 17, sous réserve des mêmes exigences que celles qui s'appliquent aux personnes physiques, qui doivent avoir commis ces infractions «intentionnellement et sans droit», et conformément aux principes juridiques de chaque État partie (paragraphes 1 et 2).

Les articles 19 et 20 reprennent les dispositions correspondantes de la convention CTO et de la CNUCC en prévoyant des règles minimales relatives à l'établissement des infractions de participation, de tentative et de préparation, ainsi qu'aux délais de prescription, conformément au droit interne des États parties et en tant que de besoin pour les infractions établies dans la convention. Bien que la transmission et le contrôle en ligne de données susceptibles d'être pertinentes dans le cadre d'une infraction reposent sur l'assistance des fournisseurs de services, un fournisseur de services qui n'a pas d'intention criminelle n'est pas tenu responsable au titre de l'article 19. Par conséquent, un fournisseur de services n'est pas tenu de surveiller activement les contenus afin d'éviter toute responsabilité pénale en application de cette disposition.

L'article 21 s'inspire également de la convention CTO et de la CNUCC; il prévoit des règles minimales relatives aux poursuites judiciaires, aux jugements et aux sanctions concernant les infractions établies conformément à la convention. Le paragraphe 4 impose aux États parties de veiller à ce que toute personne poursuivie pour une infraction établie conformément à la convention bénéficie de tous les droits et garanties dans le respect des obligations internationales applicables qui leur incombent, y compris le droit à un procès équitable et les droits de la défense.

Compétence [chapitre III (article 22)]

L'article 22 reflète également les dispositions correspondantes de la convention CTO, de la CNUCC et de la convention de Budapest et réglemente l'établissement de formes de compétence obligatoires et facultatives, selon que de besoin, à l'égard des infractions établies conformément à la convention.

Mesures procédurales et détection et répression [chapitre IV (articles 23 à 34)]

L'article 23 détermine le champ d'application des pouvoirs et des mesures procédurales internes qui permettent la coopération internationale: ces pouvoirs et mesures s'appliquent à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies conformément à la convention et les autres infractions pénales commises au moyen de systèmes d'information et de communication, ainsi qu'à la collecte des preuves sous forme électronique de toute infraction pénale. Selon les notes interprétatives sur certains articles de

la convention, qui sont annexées à la résolution portant adoption de la convention, «[l]e terme "enquêtes pénales" englobe les situations où il existe des motifs raisonnables de croire, sur la base de circonstances factuelles, qu'une infraction pénale (y compris une infraction visée à l'article 19 de la Convention) a été commise ou est en cours de commission, y compris lorsque l'enquête vise à stopper ou à empêcher la commission de l'infraction en question». Ainsi, la convention ne fournit pas de base pour la coopération internationale à des fins préventives et les données ne peuvent être échangées que si elles se rapportent à une enquête pénale spécifique.

L'article 24 reprend, avec quelques modifications, le libellé correspondant de l'article 15 de la convention de Budapest. Il prévoit des conditions et des garanties générales visant à faire en sorte que les pouvoirs et procédures prévus au chapitre IV soient soumis à un niveau approprié de protection des droits fondamentaux, y compris l'application du principe de proportionnalité. Ces conditions et garanties comprennent, entre autres, un contrôle juridictionnel ou une autre forme de contrôle indépendant, le droit à un recours efficace, des motifs justifiant l'application et la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question. En outre, les conditions et garanties mises en place conformément à cet article s'appliquent au niveau interne aux pouvoirs et procédures visés au chapitre IV, à la fois aux fins des enquêtes et des procédures pénales internes et aux fins de la coopération internationale accordée par l'État partie requis en application du chapitre V.

Les articles 25 à 30 s'inspirent des pouvoirs et des mesures procédurales internes correspondants de la convention de Budapest. Ils concernent la préservation accélérée de données électroniques stockées, la préservation et la divulgation partielle accélérées de données de trafic, l'injonction de produire, la perquisition et la saisie de données électroniques stockées, la collecte en temps réel de données de trafic et l'interception de données de contenu.

L'article 31 reflète l'article 31 de la CNUCC. Il impose aux États parties d'adopter des mesures permettant le gel, la saisie et la confiscation du produit du crime.

L'article 32 s'inspire de la convention CTO et de la CNUCC et prévoit la possibilité pour les États parties d'établir des antécédents judiciaires afin d'utiliser ces informations dans le cadre d'une procédure pénale relative à une infraction établie conformément à la convention.

L'article 33 s'inspire de la convention CTO et impose aux États parties de prendre, conformément à leur droit interne, des mesures appropriées pour assurer une protection adéquate aux témoins.

L'article 34 s'inspire de la convention CTO et impose aux États parties de prendre, conformément à leur droit interne, des mesures appropriées pour apporter une assistance adéquate aux victimes, en particulier aux victimes des infractions établies aux articles 14 à 16 de la convention. Lorsqu'ils donnent suite aux dispositions de ses paragraphes 2 à 4, l'article 34 impose également aux États parties de tenir compte de l'âge, du genre et de la situation et des besoins particuliers des victimes, y compris de la situation et des besoins particuliers des enfants. Dans la mesure où cela est compatible avec leur cadre juridique interne, le paragraphe 6 encourage les États parties à prendre des dispositions concrètes pour qu'il soit satisfait aux demandes visant à ce que le contenu décrit aux articles 14 et 16 de la convention soit retiré ou rendu inaccessible.

Coopération internationale [chapitre V (articles 35 à 52)]

L'article 35 définit les principes généraux et le champ d'application de la coopération internationale, qui impose aux États parties de coopérer entre eux aux fins des enquêtes et des poursuites concernant les infractions pénales établies conformément à la convention et de la

collecte et de la communication de preuves électroniques desdites infractions, ainsi que de la collecte et de la communication de preuves électroniques de toute infraction grave passible d'une peine privative de liberté maximale d'au moins quatre ans ou d'une peine plus grave. Par conséquent, le champ d'application de la coopération internationale est limité aux infractions établies conformément à la convention et aux infractions graves avec un seuil de peine clair.

L'article 36 contient une disposition explicite sur la protection des données personnelles. Cette disposition fixe les règles relatives au transfert de données personnelles dans le cadre de la coopération internationale. Le transfert ne peut avoir lieu que conformément au droit interne et aux obligations de droit international de l'État partie procédant au transfert. Les États parties peuvent refuser de transférer des données personnelles si cela ne peut pas être fait conformément à leurs lois applicables concernant la protection des données personnelles. Pour l'UE, cela signifie que des principes importants en matière de protection des données, notamment la limitation des finalités, la minimisation des données, la proportionnalité et la nécessité, doivent être appliqués, conformément à la charte des droits fondamentaux de l'Union européenne, avant que toute donnée à caractère personnel puisse être communiquée à un autre État partie. Les États parties peuvent également exiger, pour donner suite à une demande de données personnelles, que soient respectées les conditions propres à assurer la conformité. Les États parties sont tenus de veiller à ce que leurs cadres juridiques respectifs prévoient l'application de garanties effectives et appropriées aux données personnelles qu'ils reçoivent en vertu de la convention. Les États parties ne peuvent transférer les données personnelles reçues à un pays tiers ou à une organisation internationale qu'avec l'autorisation préalable de l'État partie ayant procédé au transfert initial, lequel peut exiger que ladite autorisation soit fournie par écrit.

L'article 37 s'inspire de la CNUCC et de la convention de Budapest et prévoit des règles détaillées en matière d'extradition. Conformément au paragraphe 8, la convention autorise le refus d'extradition sur la base des conditions prévues par le droit national de l'État partie requis. Le paragraphe 15 établit un autre motif de refus d'une demande d'extradition, dans les cas où la demande a été présentée aux fins de poursuivre ou de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politiques, ou dans ceux où donner suite à la demande causerait un préjudice à cette personne pour l'une quelconque de ces raisons.

Les articles 38 et 39 s'inspirent de la convention CTO et de la CNUCC et prévoient une possibilité de transfèrement des personnes condamnées et de transfert des procédures pénales.

L'article 40 fait écho aux dispositions de la convention CTO, de la CNUCC et de la convention de Budapest et définit des dispositions détaillées sur les principes et procédures d'entraide judiciaire. Le paragraphe 17 exige que les demandes d'entraide judiciaire soient exécutées conformément au droit interne de l'État partie requis. Le paragraphe 19 interdit à un État partie requérant de communiquer ou d'utiliser les informations ou les preuves fournies par l'État partie requis pour des enquêtes, poursuites ou procédures judiciaires autres que celles visées dans la demande sans le consentement préalable de l'État partie requis. Les paragraphes 8, 21 et 22 prévoient de vastes motifs de refus des demandes d'entraide judiciaire, comme décrit dans la section «*Droits fondamentaux*».

L'article 41 s'inspire de l'article 35 de la convention de Budapest et impose aux États parties de mettre en place des réseaux 24/7 afin d'assurer une assistance pour des enquêtes, des poursuites ou des procédures judiciaires spécifiques concernant des infractions établies conformément à la convention ou pour la collecte de preuves électroniques.

Les articles 42 à 46 font écho aux articles 29 à 33 de la convention de Budapest et détaillent des types spécifiques de mesures de coopération internationale en matière d'entraide judiciaire. Ces mesures sont la préservation accélérée de données électroniques stockées, la divulgation accélérée de données de trafic préservées, l'accès aux données électroniques stockées, la collecte en temps réel de données de trafic et l'interception de données de contenu. En ce qui concerne les mesures les plus intrusives que sont la collecte en temps réel de données de trafic et l'interception de données de contenu, les États parties ont une obligation plus limitée de «s'efforcer» de fournir une telle aide. Cette obligation constitue en substance une «obligation de moyens» et est donc moins contraignante pour les États parties que les obligations relatives aux autres mesures d'entraide judiciaire, qui imposent de coopérer avec les autres États parties à moins que les conditions applicables ne soient pas remplies ou que l'un des motifs de refus applicables ne soit invoqué. En outre, l'aide aux fins de l'interception de données de contenu ne peut être demandée que pour des infractions pénales graves dans la mesure permise par les traités applicables aux États parties ou par le droit interne de ces derniers.

Les articles 47 et 48 s'inspirent de la convention CTO et de la CNUCC et encouragent les États parties à coopérer en vue de renforcer la détection et la répression des infractions établies conformément à la convention et à établir des instances d'enquête conjointes à cette fin.

Les articles 49 à 52 s'inspirent de la convention CTO et/ou de la CNUCC et prévoient des règles minimales concernant les mesures de confiscation, de recouvrement et de restitution du produit des infractions établies conformément à la convention ou des biens connexes.

Mesures préventives [chapitre VI (article 53)]

L'article 53 encourage les États parties à s'efforcer, conformément aux principes fondamentaux de leurs systèmes juridiques, d'élaborer et de mettre en œuvre ou de maintenir des politiques et des bonnes pratiques efficaces et coordonnées afin de réduire, par des mesures législatives, administratives ou autres appropriées, les possibilités actuelles ou futures de cybercriminalité. Les États parties devraient favoriser la participation active des personnes et des entités n'appartenant pas au secteur public, telles que les organisations non gouvernementales, les organisations de la société civile, les établissements universitaires et les entités du secteur privé, concernées, ainsi que du grand public, aux aspects pertinents de la prévention des infractions établies conformément à la convention. Le paragraphe 3 fournit une liste non exhaustive et non contraignante de mesures préventives. Le paragraphe 3, alinéa e), fait explicitement référence aux mesures préventives reconnaissant les contributions qu'apportent, par leurs activités légitimes, les personnes qui conduisent des recherches dans le domaine de la sécurité lorsque celles-ci ont pour seul but de renforcer et d'améliorer la sécurité des produits, des services et de la clientèle des fournisseurs de services.

Assistance technique et échange d'informations [chapitre VII (articles 54 à 56)]

Les articles 54 à 56 s'inspirent de la convention CTO et/ou de la CNUCC et énoncent des dispositions relatives à la fourniture d'une assistance technique, au renforcement des capacités et à l'échange d'informations, en tenant compte tout particulièrement des intérêts et des besoins des États parties en développement.

Mécanisme d'application [chapitre VIII (articles 57 à 58)]

Les articles 57 et 58 s'inspirent de la CNUCC et donnent des précisions sur la conférence des États parties, qui supervisera la mise en œuvre de la convention et sera compétente pour élaborer et adopter des protocoles additionnels à la convention sur la base des articles 61 et 62 de celle-ci. Le secrétaire général ou la secrétaire générale de l'Organisation des Nations unies

fournit les services de secrétariat et convoque la conférence des États parties au plus tard un an après l'entrée en vigueur de la convention. Par la suite, la conférence tient des réunions ordinaires conformément au règlement intérieur qu'elle a adopté.

Dispositions finales [chapitre IX (articles 59 à 68)]

Le chapitre IX de la convention contient les dispositions finales. L'article 60, paragraphe 1, garantit notamment que les États membres de l'UE qui sont parties à la convention peuvent continuer à appliquer le droit de l'Union dans leurs relations mutuelles. Il permet également aux parties à la convention de Budapest et à d'autres instruments internationaux de continuer à appliquer ces instruments entre elles.

L'article 64, paragraphe 1, dispose que la convention est ouverte à la signature de tous les États à Hanoï en octobre 2025, puis au siège de l'Organisation des Nations unies, à New York, jusqu'au 31 décembre 2026. Conformément au paragraphe 2, la convention est également ouverte à la signature des organisations régionales d'intégration économique, telles que l'Union, à la condition qu'au moins un État membre d'une telle organisation l'ait signée conformément au paragraphe 1.

L'article 64, paragraphe 3, et l'article 65, paragraphe 1, indiquent que la convention entrera en vigueur dès que 40 États auront exprimé leur consentement à être liés par elle en déposant leurs instruments de ratification, d'acceptation ou d'approbation auprès du secrétaire général ou de la secrétaire générale de l'Organisation des Nations unies. Des organisations régionales d'intégration économique, telles que l'Union, peuvent déposer leur instrument de ratification, d'acceptation ou d'approbation si au moins un de leurs États membres l'a fait. Dans cet instrument de ratification, d'acceptation ou d'approbation, l'organisation régionale d'intégration économique déclare l'étendue de sa compétence concernant les questions régies par la convention. Conformément à l'article 64, paragraphe 4, la convention est ouverte à l'adhésion d'organisations régionales d'intégration économique, telles que l'Union, à condition qu'au moins un État membre de l'organisation concernée soit partie à la convention. Au moment de son adhésion, l'Union doit déclarer l'étendue de sa compétence concernant les questions régies par la convention.

Conformément à l'article 66, paragraphe 1, à l'expiration d'un délai de cinq ans à compter de l'entrée en vigueur de la convention, un État partie peut proposer un amendement et le transmettre au secrétaire général ou à la secrétaire générale de l'Organisation des Nations unies, qui communique alors la proposition d'amendement aux États parties et à la conférence des États parties à la convention en vue de l'examen de la proposition et de l'adoption d'une décision. Sur la base du paragraphe 2, les organisations régionales d'intégration économique, telles que l'Union, disposent, pour exercer leur droit de vote dans les domaines qui relèvent de leur compétence, d'un nombre de voix égal au nombre de leurs États membres parties à la convention. Un amendement adopté conformément au paragraphe 1 est soumis à ratification, acceptation ou approbation des États parties.

Les articles 61 et 62 prévoient des règles relatives aux protocoles additionnels à la convention. L'article 61, paragraphe 2, autorise les organisations régionales d'intégration économique, telles que l'Union, à devenir partie à un protocole uniquement si l'organisation est partie à la convention. Conformément au paragraphe 4, tout protocole à la convention doit être interprété conjointement avec la convention, compte tenu de l'objet de ce protocole. L'article 62, paragraphe 1, exige au moins 60 États parties pour que la conférence des États parties envisage l'adoption d'un protocole additionnel. Cet article prévoit également que la conférence des États parties n'épargne aucun effort pour parvenir à un consensus sur tout protocole additionnel et indique que, seulement si tous les efforts en ce sens ont été épuisés, il faut, en dernier recours, pour que le protocole additionnel soit adopté, un vote à la majorité

des deux tiers au moins des États parties présents à la réunion de la conférence des États parties et exprimant leur vote. Conformément à l'article 62, paragraphe 2, les organisations régionales d'intégration économique, telles que l'Union, disposent, pour exercer, en vertu dudit article, leur droit de vote dans les domaines qui relèvent de leur compétence, d'un nombre de voix égal au nombre de leurs États membres parties à la convention.

Conformément à l'article 67, paragraphe 2, les organisations régionales d'intégration économique, telles que l'Union, cessent d'être parties à la convention lorsque tous leurs États membres l'ont dénoncée.

La résolution portant adoption de la convention est accompagnée de notes interprétatives relatives aux articles 2, 17, 23 et 35. Bien que ces notes interprétatives ne constituent pas un instrument donnant une interprétation de la convention faisant autorité, elles sont destinées à guider et à aider les parties dans son application. Les notes interprétatives de la présidence du comité spécial des Nations unies distribuées au cours des négociations abordent également plusieurs aspects essentiels de l'interprétation. Le site web du comité spécial, sur lequel toutes les propositions et révisions du projet de texte de la convention présentées au cours des négociations sont disponibles, fournit des informations utiles sur l'élaboration des dispositions essentielles du texte et peut avoir une valeur interprétative. En outre, le rapport explicatif de la convention de Budapest[24], même s'il est informel, peut également constituer un outil d'information utile pour les États en ce qui concerne les nombreuses dispositions inspirées de la convention de Budapest, telles que la plupart des dispositions de la convention relatives à l'incrimination et aux pouvoirs procéduraux.

[24] Série des traités européens — nº 185.

2025/0230 (NLE)

Proposition de

DÉCISION DU CONSEIL

relative à la signature, au nom de l'Union européenne, de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves»

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16, son article 82, paragraphe 1, son article 83, paragraphe 1, et son article 87, paragraphe 2, en liaison avec son article 218, paragraphe 5,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Le 24 mai 2022, la décision (UE) 2022/895 du Conseil a autorisé la Commission à participer, au nom de l'Union européenne, aux négociations en vue d'une convention des Nations unies contre la cybercriminalité.

(2) Le texte de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves» (ci-après la «convention») a été adopté par l'Assemblée générale des Nations unies le 24 décembre 2024 et devrait être ouvert à la signature à Hanoï, au Viêt Nam, le 25 octobre 2025, puis au siège des Nations unies, à New York, jusqu'au 31 décembre 2026.

(3) La convention est conforme aux objectifs de sécurité de l'Union européenne visés à l'article 67, paragraphe 3, du traité sur le fonctionnement de l'Union européenne, à savoir assurer un niveau élevé de sécurité par des mesures de prévention de la criminalité ainsi que de lutte contre celle-ci, par des mesures de coordination et de coopération entre les autorités policières et judiciaires et autres autorités compétentes, ainsi que par le rapprochement des législations pénales.

(4) Les dispositions de la convention s'appliquent à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales établies conformément à la convention et ne permettent l'échange de données qu'à cette fin.

(5) La convention harmonise un ensemble limité d'infractions clairement définies tout en laissant aux États parties la souplesse nécessaire pour éviter une incrimination excessive d'actes légitimes.

(6) La convention n'établit que des règles minimales relatives à la responsabilité des personnes morales pour les infractions qui y sont visées et n'exige pas d'établir cette responsabilité pénale d'une manière qui serait incompatible avec les principes juridiques d'un État partie.

(7) La convention est également conforme aux objectifs de l'Union européenne en matière de protection des données à caractère personnel, de la vie privée et des droits fondamentaux, tels que visés à l'article 16 du traité sur le fonctionnement de l'Union européenne et dans la charte des droits fondamentaux de l'Union européenne.

(8) La convention prévoit des garanties solides en matière de droits de l'homme et exclut toute interprétation qui conduirait à réprimer les droits de l'homme ou les libertés fondamentales, notamment la liberté d'expression, de conscience, d'opinion, de religion ou de conviction, de réunion pacifique et d'association. Ces garanties permettent également de refuser la coopération internationale si elle est contraire au droit interne des États parties ou si cela est nécessaire pour éviter toute forme de discrimination.

(9) En ce qui concerne les pouvoirs et les mesures procédurales au niveau tant interne qu'international, la convention prévoit des conditions et des garanties horizontales qui assurent la protection des droits de l'homme, conformément aux obligations incombant aux États parties en vertu du droit international des droits de l'homme, et qui intègrent le principe de proportionnalité. Ces conditions et garanties comprennent, entre autres, un contrôle juridictionnel ou une autre forme de contrôle indépendant, le droit à un recours efficace, des motifs justifiant l'application et la limitation du champ d'application et de la durée des pouvoirs et des procédures.

(10) La convention comprend une disposition spécifique sur la protection des données à caractère personnel qui garantit que des principes importants en matière de protection des données, notamment la limitation des finalités, la minimisation des données, la proportionnalité et la nécessité, doivent être appliqués, conformément à la charte des droits fondamentaux de l'Union européenne, avant que toute donnée à caractère personnel puisse être communiquée à un autre État partie.

(11) En participant aux négociations au nom de l'Union, la Commission a veillé à la compatibilité de la convention avec les règles pertinentes de l'Union européenne.

(12) Un certain nombre de réserves et de notifications sont nécessaires pour garantir la compatibilité de la convention avec le droit et les politiques de l'Union, l'application uniforme de la convention par les différents États membres dans leurs relations avec les États parties non membres de l'UE, ainsi que l'application effective de la convention.

(13) Les réserves et les notifications au sujet desquelles des orientations sont fournies à l'annexe I de la présente décision sont sans préjudice de toute autre réserve ou déclaration que les États membres pourraient souhaiter exprimer ou soumettre individuellement lorsque cela est autorisé.

(14) Dans la mesure où la convention prévoit des procédures améliorant l'accès transfrontière aux preuves électroniques et un niveau élevé de garanties, le fait de devenir partie à celle-ci favorisera la cohérence des efforts déployés par l'Union européenne pour lutter contre la cybercriminalité et d'autres formes de criminalité au niveau mondial. Il facilitera la coopération entre les parties à la convention qui sont des États membres de l'UE et celles qui ne le sont pas, tout en assurant un niveau élevé de protection des personnes.

(15) Conformément à son article 64, la convention est ouverte à la signature de l'Union.

(16) L'Union devrait devenir partie à la convention aux côtés de ses États membres, étant donné que l'une comme les autres disposent de compétences dans les domaines couverts par la convention. La présente décision est sans préjudice de la signature de la convention par les États membres, conformément à leurs procédures internes.

(17) La signature rapide de la convention par l'Union européenne permettra en outre à cette dernière de faire entendre sa voix dès le début de la mise en œuvre de ce nouveau cadre mondial de lutte contre la cybercriminalité.

(18) 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 [...].

(19) [Conformément à l'article 3 du protocole nº 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, l'Irlande a notifié [, *par une lettre du* …,] son souhait de participer à l'adoption et à l'application de la présente décision.]

OU

[Conformément aux articles 1er et 2 du protocole nº 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.]

(20) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Royaume de Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Royaume de Danemark ne participe pas à l'adoption de la présente décision et n'est pas lié par celle-ci ni soumis à son application.

(21) Il convient de signer la convention et d'approuver les réserves et notifications ci-jointes,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La signature de la convention des Nations unies contre la cybercriminalité intitulée «Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves» (ci-après la «convention») est autorisée au nom de l'Union européenne, sous réserve de la conclusion de ladite convention.

Le texte de la convention est joint à la présente décision (annexe II).

Article 2

Les réserves et notifications qui figurent à l'annexe I de la présente décision sont approuvées.

Article 3

La présente décision entre en vigueur le jour suivant celui de son adoption.

Fait à Bruxelles, le

Par le Conseil
Le président
[...]