COM(2021) 718 final

ASSEMBLÉE NATIONALE
QUINZIÈME LÉGISLATURE

SÉNAT
SESSION ORDINAIRE DE 2021-2022

Reçu à la Présidence de l'Assemblée nationale
le 07 décembre 2021

Enregistré à la Présidence du Sénat
le 07 décembre 2021

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 autorisant les États membres à signer, dans lìntérêt de lUnion européenne, le deuxième protocole additionnel à la convention sur la cybercriminalité relative au renforcement de la coopération et de la divulgation de preuves électroniques

E16278

Conseil de
l'Union européenne

Bruxelles, le 2 décembre 2021
(OR. en)

14612/21

Dossier interinstitutionnel:
2021/0382(NLE)

JAI 1332
COPEN 432
CYBER 320
ENFOPOL 482
TELECOM 452
EJUSTICE 105
MI 912
DATAPROTECT 276

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	25 novembre 2021
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2021) 718 final
Objet:	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

Les délégations trouveront ci-joint le document COM(2021) 718 final.

p.j.: COM(2021) 718 final

COMMISSION
EUROPÉENNE

Bruxelles, le 25.11.2021
COM(2021) 718 final

2021/0382 (NLE)

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

EXPOSÉ DES MOTIFS

1. OBJET DE LA PROPOSITION

La présente proposition concerne la décision autorisant les États membres à signer, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la Convention de Budapest du Conseil de l'Europe sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (ci-après le «protocole»)[1]. Le protocole a pour objet d'établir des règles communes au niveau international afin de renforcer la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique pour les enquêtes ou procédures pénales.

La Commission présentera également une proposition de décision du Conseil de l'Union européenne (ci-après le «Conseil») autorisant les États membres à ratifier le protocole dans l'intérêt de l'Union européenne.

La cybercriminalité continue de représenter un défi considérable pour notre société. En dépit des efforts déployés par les services répressifs et les autorités judiciaires, les cyberattaques, y compris les attaques par logiciel rançonneur, se multiplient et se complexifient[2]. 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 différents pays.

Les preuves électroniques revêtent une importance croissante pour les enquêtes pénales. La Commission estime qu'à l'heure actuelle, les services répressifs et les autorités judiciaires ont besoin d'avoir accès à des preuves électroniques dans 85 % des enquêtes pénales, y compris en matière de cybercriminalité[3]. Les preuves d'infractions pénales étant de plus en plus détenues sous forme électronique par des fournisseurs de services sur le territoire de juridictions étrangères et, pour permettre une réponse effective de la justice pénale, il est nécessaire d'obtenir ces preuves par des mesures appropriées afin de défendre l'état de droit.

Des efforts visant à améliorer l'accès transfrontière aux preuves électroniques pour les enquêtes pénales sont déployés dans le monde entier, au niveau national, de l'Union européenne[4] et international, y compris grâce au protocole. Il importe de garantir la compatibilité des règles au niveau international afin d'éviter les conflits de lois lorsqu'un accès transfrontière à des preuves électroniques est sollicité.

2. CONTEXTE DE LA PROPOSITION

2.1. Contexte

La convention de Budapest du Conseil de l'Europe sur la cybercriminalité (STCE nº 185) (ci-après la «convention») a pour objectif de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques. 1) Elle contient des dispositions harmonisant les éléments constitutifs des infractions en droit pénal matériel national et des dispositions connexes dans le domaine de la cybercriminalité, 2) elle prévoit les pouvoirs nécessaires en

[1] Le texte du protocole figurera en annexe de la proposition de décision du Conseil autorisant les États membres à ratifier, dans l'intérêt de l'Union européenne, le protocole.

[2] Évaluation 2021 de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE 2021).

[3] SWD(2018) 118 final.

[4] COM(2018) 225 et 226 final.

droit pénal procédural national pour les enquêtes et les poursuites concernant ces infractions ainsi que d'autres infractions commises au moyen d'un système informatique ou dont les preuves revêtent une forme électronique, et 3) elle vise à mettre en place un système rapide et efficace de coopération internationale.

La convention est ouverte aux États membres du Conseil de l'Europe et aux pays tiers sur invitation. 66 pays sont actuellement parties à la convention, y compris 26 États membres de l'Union européenne[5]. La convention ne prévoit pas que l'Union européenne puisse adhérer à la convention. L'Union européenne est toutefois reconnue comme une organisation ayant le statut d'observateur au sein du comité de la convention sur la cybercriminalité (T-CY)[6].

Bien que des efforts soient déployés pour négocier une nouvelle convention sur la cybercriminalité au niveau des Nations unies[7], la convention de Budapest demeure la principale convention multilatérale pour la lutte contre la cybercriminalité. L'Union soutient de manière constante la convention[8], également dans le cadre du financement de programmes de renforcement des capacités[9].

À la suite de propositions du groupe sur les preuves en nuage[10], le comité de la convention sur la cybercriminalité a adopté plusieurs recommandations visant à remédier – notamment en négociant un deuxième protocole additionnel à la convention sur la cybercriminalité relatif à la coopération internationale renforcée – au problème lié au fait que les preuves électroniques concernant la cybercriminalité et d'autres infractions sont de plus en plus détenues par des fournisseurs de services sur le territoire de juridictions étrangères, tandis que les pouvoirs des services répressifs restent limités par les frontières territoriales. En juin 2017, le comité de la convention sur la cybercriminalité a approuvé le mandat pour la préparation d'un deuxième protocole additionnel à la convention au cours de la période de septembre 2017 à décembre 2019[11]. Compte tenu de la nécessité de disposer de plus de temps pour achever les discussions, ainsi que des contraintes imposées par la pandémie de COVID-19 en 2020 et 2021, le comité de la convention sur la cybercriminalité a ensuite prorogé ce mandat à deux reprises, jusqu'en décembre 2020, puis jusqu'en mai 2021.

À la suite de l'appel lancé par le Conseil européen dans ses conclusions du 18 octobre 2018[12], la Commission a adopté, le 5 février 2019, une recommandation de décision du Conseil autorisant la Commission à participer, au nom de l'Union européenne, aux négociations relatives à un deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité[13]. Le 2 avril 2019, le contrôleur européen de la protection des données a

---

5 Tous sauf l'Irlande, qui a signé mais pas ratifié la convention, tout en s'étant engagée à y adhérer.

6 Règlement intérieur du comité de la convention sur la cybercriminalité [T-CY (2013)25 rev], disponible à l'adresse suivante: www.coe.int/cybercrime.

7 Résolution 74/247 de l'Assemblée générale des Nations unies (AGNU) de décembre 2019 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

8 JOIN(2020) 81 final.

9 Voir, par exemple, l'action globale sur la cybercriminalité élargie (GLACY+), à l'adresse suivante: https://www.coe.int/fr/web/cybercrime/glacyplus

10 Rapport final du groupe sur les preuves dans le nuage du comité de la convention sur la cybercriminalité intitulé «Accès de la justice pénale aux preuves électroniques dans le cloud: Recommandations pour examen par le T-CY», du 16 septembre 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

12 https://www.consilium.europa.eu/fr/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

adopté un avis sur cette recommandation[14]. Par décision du 6 juin 2019, le Conseil de l'Union européenne a autorisé la Commission à participer, au nom de l'Union européenne, aux négociations relatives au deuxième protocole additionnel[15].

Comme indiqué dans la stratégie 2020 de l'UE pour l'union de la sécurité[16], la stratégie 2020 de cybersécurité de l'UE pour la décennie numérique[17] et la stratégie 2021 de l'UE visant à lutter contre la criminalité organisée[18], la Commission s'est engagée à assurer une conclusion rapide et fructueuse des négociations sur le protocole. Le Parlement européen a également reconnu la nécessité de conclure les travaux sur le protocole dans sa résolution de 2021 sur la stratégie de cybersécurité de l'Union pour la décennie numérique[19].

La Commission a participé, au nom de l'Union européenne, aux négociations relatives au protocole conformément à la décision du Conseil de l'Union européenne. La Commission a régulièrement consulté le comité spécial du Conseil pour les négociations au sujet de la position de l'Union.

Conformément à l'accord-cadre sur les relations entre le Parlement européen et la Commission européenne[20], la Commission a également tenu le Parlement européen informé des négociations au moyen de rapports écrits et de présentations orales.

Lors de la réunion plénière du 28 mai 2021, le comité de la convention sur la cybercriminalité a approuvé le projet de protocole à son niveau et a transmis ce projet pour adoption par le Comité des ministres du Conseil de l'Europe[21]. Le 17 novembre 2021, le Comité des ministres du Conseil de l'Europe a adopté le protocole.

2.2. Deuxième protocole additionnel

L'objectif du protocole est de renforcer la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques. Le protocole reconnaît la nécessité d'une coopération accrue et plus efficace entre les États et le secteur privé et d'une plus grande clarté ou sécurité juridique pour les fournisseurs de services et autres entités concernant les circonstances dans lesquelles ils peuvent répondre à des demandes de divulgation de preuves électroniques émanant des autorités de justice pénale d'autres parties.

Le protocole reconnaît également que des conditions et garanties effectives en matière de protection des droits fondamentaux sont indispensables pour une coopération transfrontière efficace aux fins de la justice pénale, y compris entre les secteurs public et privé. À cette fin, le protocole suit une approche fondée sur les droits et prévoit des conditions et des garanties conformes aux instruments internationaux en matière de droits de l'homme, y compris la convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de

[14] Avis 3/2019 du CEPD du 2 avril 2019 relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité.
[15] Décision du Conseil portant la référence 9116/19.
[16] COM(2020) 605 final.
[17] JOIN(2020) 81 final.
[18] COM(2021) 170 final.
[19] Résolution du Parlement européen du 10 juin 2021 sur la stratégie de cybersécurité de l'Union pour la décennie numérique.
[20] Référence L 304/47.
[21] https://rm.coe.int/0900001680a2aa42

l'Europe de 1950. Étant donné que les preuves électroniques concernent souvent des données à caractère personnel, le protocole prévoit également des garanties solides pour la protection de la vie privée et des données à caractère personnel.

Les dispositions mentionnées dans les sous-sections suivantes revêtent une importance particulière pour le protocole. Le protocole est accompagné d'un rapport explicatif détaillé. Bien que ce rapport explicatif ne constitue pas un instrument donnant une interprétation du protocole faisant autorité, il est destiné «à guider et à aider les parties» dans l'application du protocole[22].

2.2.1. Dispositions communes

Le chapitre I du protocole prévoit des dispositions communes. L'article 2 détermine le champ d'application du protocole, conformément à la portée de la convention: celui-ci s'applique à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique.

L'article 3 comprend les définitions des termes «autorité centrale», «autorité compétente», «urgence», «données à caractère personnel» et «partie transférante». Ces définitions s'appliquent au protocole, de même que les définitions figurant dans la convention.

L'article 4 détermine les langues dans lesquelles les parties doivent présenter les injonctions, les demandes ou les notifications au titre du protocole.

2.2.2. Mesures de coopération

Le chapitre II du protocole prévoit des dispositions pour renforcer la coopération. Tout d'abord, l'article 5, paragraphe 1, prévoit que les parties s'assurent la coopération mutuelle la plus large possible. L'article 5, paragraphes 2 à 5, détermine l'application des mesures du protocole par rapport aux traités ou arrangements d'entraide existants. L'article 5, paragraphe 7, indique que les mesures visées au chapitre II ne restreignent pas la coopération entre les parties, ou entre les parties et les fournisseurs de services ou d'autres entités, par le biais d'autres accords, arrangements, pratiques ou le droit interne applicables.

L'article 6 offre une base pour la coopération directe entre les autorités compétentes sur le territoire d'une partie et les entités fournissant des services d'enregistrement de noms de domaine sur le territoire d'une autre partie, en vue de la divulgation de données relatives à l'enregistrement de noms de domaine.

L'article 7 offre une base pour la coopération directe entre les autorités compétentes sur le territoire d'une partie et les fournisseurs de services sur le territoire d'une autre partie, en vue de la divulgation de données relatives aux abonnés.

L'article 8 offre une base en vue du renforcement de la coopération entre autorités pour la divulgation de données informatiques.

L'article 9 offre une base en vue de la coopération entre autorités pour la divulgation de données informatiques en situation d'urgence.

---

[22] Voir le paragraphe 2 du rapport explicatif du protocole.

L’article 10 offre une base pour l’entraide judiciaire en situation d’urgence.

L’article 11 offre une base pour la coopération par vidéoconférence.

L’article 12 offre une base pour les enquêtes communes et les équipes communes d’enquête.

2.2.3. Garanties

Le protocole suit une approche fondée sur les droits, assortie de conditions et de garanties spécifiques, dont certaines sont intégrées dans les mesures de coopération spécifiques ainsi que dans le chapitre III du protocole. L’article 13 du protocole impose aux parties de veiller à ce que les pouvoirs et les procédures soient soumis à un niveau adéquat de protection des droits fondamentaux, ce qui, conformément à l’article 15 de la convention, garantit l’application du principe de proportionnalité.

L’article 14 du protocole prévoit la protection des données à caractère personnel, telles que définies à l’article 3 du protocole, conformément au protocole d’amendement à la convention pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel (STCE nº 223) (convention 108+) et au droit de l’Union.

Sur cette base, l’article 14, paragraphes 2 à 15, énonce les principes fondamentaux en matière de protection des données, y compris la limitation au regard de la finalité, la base juridique, la qualité des données et les règles applicables au traitement de catégories particulières de données, les obligations applicables aux responsables du traitement, notamment pour la conservation, la tenue de registres, la sécurité et les transferts ultérieurs, les droits individuels opposables, y compris en ce qui concerne la notification, l’accès, la rectification et la prise de décision automatisée, la supervision indépendante et effective par une ou plusieurs autorités ainsi que les recours administratifs et judiciaires. Les garanties couvrent toutes les formes de coopération présentées dans le protocole, moyennant des adaptations, s’il y a lieu, pour tenir compte des spécificités de la coopération directe (par exemple, dans le contexte de la notification d’une violation). L’exercice de certains droits individuels peut être retardé, limité ou refusé lorsque cela est nécessaire et proportionné pour poursuivre des objectifs d’intérêt public importants, en particulier pour éviter de mettre en péril une enquête en cours menée par des services répressifs, ce qui est également conforme au droit de l’Union.

L’article 14 du protocole devrait également être lu en liaison avec l’article 23 du protocole. L’article 23 renforce l’effectivité des garanties prévues par le protocole en prévoyant que le comité de la convention sur la cybercriminalité évaluera la mise en œuvre et l’application des mesures prises dans la législation nationale pour donner effet aux dispositions du protocole. En particulier, l’article 23, paragraphe 3, reconnaît explicitement que la mise en œuvre par les parties de l’article 14 sera évaluée dès que dix parties à la convention auront exprimé leur consentement à être liées par le protocole.

À titre de garantie supplémentaire, conformément à l’article 14, paragraphe 15, lorsqu’une partie dispose de preuves substantielles qu’une autre partie viole de manière systématique ou flagrante les garanties énoncées dans le protocole, elle peut suspendre le transfert de données à caractère personnel vers cette partie après consultation (laquelle n’est pas exigée en cas d’urgence). Toutes les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au protocole.

Enfin, compte tenu du caractère multilatéral du protocole, l'article 14, paragraphe 1, points b) et c), du protocole permet aux parties, dans le cadre de leurs relations bilatérales, de convenir, sous certaines conditions, d'autres moyens d'assurer la protection des données à caractère personnel transférées en vertu du protocole. Si les garanties prévues à l'article 14, paragraphes 2 à 15, s'appliquent par défaut aux parties recevant des données à caractère personnel, sur la base de l'article 14, paragraphe 1, point b), les parties liées mutuellement par un accord international établissant un cadre global pour la protection des données à caractère personnel, conformément aux exigences applicables de la législation des parties concernées, peuvent également s'appuyer sur ce cadre. Il s'agit par exemple de la convention 108+ (pour les parties qui autorisent les transferts de données vers d'autres parties en vertu de cette convention) ou de l'accord-cadre UE-États-Unis (dans le cadre de son champ d'application, c'est-à-dire pour le transfert de données à caractère personnel entre autorités et, en combinaison avec un accord spécifique de transfert entre les États-Unis et l'UE, pour la coopération directe entre les autorités et les fournisseurs de services). En outre, sur la base de l'article 14, paragraphe 1, point c), les parties peuvent également déterminer d'un commun accord que le transfert de données à caractère personnel a lieu sur la base d'autres accords ou arrangements entre les parties concernées. En ce qui concerne les États membres de l'UE, un autre accord ou arrangement de ce type ne peut être invoqué pour les transferts de données au titre du protocole que si ces transferts sont conformes aux exigences du droit de l'Union en matière de protection des données, à savoir le chapitre V de la directive (UE) 2016/680 (directive dans le domaine répressif) et (pour la coopération directe entre autorités et fournisseurs de services en vertu des articles 6 et 7 du protocole) le chapitre V du règlement (UE) 2016/679 (règlement général sur la protection des données).

2.2.4. Dispositions finales

Le chapitre IV du protocole comprend les dispositions finales. Entre autres, l'article 15, paragraphe 1, point a), garantit que les parties peuvent établir leurs relations concernant les questions traitées dans le protocole conformément à l'article 39, paragraphe 2, de la convention. L'article 15, paragraphe 1, point b), garantit que les États membres de l'UE qui sont parties au protocole peuvent continuer à appliquer le droit de l'Union dans leurs relations mutuelles. L'article 15, paragraphe 2, dispose également que l'article 39, paragraphe 3, de la convention s'applique au protocole.

L'article 16, paragraphe 3, indique que le protocole entrera en vigueur après que cinq parties à la convention auront exprimé leur consentement à être liées par le protocole.

L'article 19, paragraphe 1, prévoit que les parties peuvent se prévaloir de la ou des réserves prévues à l'article 7, paragraphe 9, points a) et b), à l'article 8, paragraphe 13, et à l'article 17. L'article 19, paragraphe 2, prévoit que les parties peuvent faire la ou les déclarations prévues à l'article 7, paragraphe 2, point b), et paragraphe 8, à l'article 8, paragraphe 11, à l'article 9, paragraphe 1, point b), et paragraphe 5, à l'article 10, paragraphe 9, à l'article 12, paragraphe 3, et à l'article 18, paragraphe 2. L'article 19, paragraphe 3, prévoit que toute partie à la convention fait toute(s) déclaration(s), notifications ou communications visées à l'article 7, paragraphe 5, points a) et e), à l'article 8, paragraphe 4 et paragraphe 10, points a) et b), à l'article 14, paragraphe 7, point c) et paragraphe 10, point b), et à l'article 17, paragraphe 2.

L'article 23, paragraphe 1, offre une base pour les consultations entre les parties, y compris par l'intermédiaire du comité de la convention sur la cybercriminalité, conformément à l'article 46 de la convention. L'article 23, paragraphe 2, offre également une base pour l'évaluation de l'utilisation et de la mise en œuvre des dispositions du protocole. L'article 23, paragraphe 3, garantit que l'examen de l'utilisation et de la mise en œuvre de l'article 14

relatif à la protection des données débute lorsque dix parties à la convention ont exprimé leur consentement à être liée par le protocole.

2.3. Droit et politique de l'Union dans le domaine

Le domaine régi par le protocole est couvert en grande partie par les règles communes fondées sur l'article 82, paragraphe 1, et l'article 16 du TFUE. Le cadre juridique actuel de l'Union européenne comprend notamment des instruments de coopération des services répressifs et judiciaires en matière pénale, tels que la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne et la décision-cadre 2002/465/JAI du Conseil relative aux équipes communes d'enquête. Sur le plan extérieur, l'Union européenne a conclu plusieurs accords bilatéraux avec des pays tiers, tels que les accords en matière d'entraide judiciaire avec, respectivement, les États-Unis d'Amérique, le Japon ainsi que la Norvège et l'Islande. L'actuel cadre juridique de l'Union européenne comprend également le règlement (UE) 2017/1939 mettant en œuvre une coopération renforcée concernant la création du Parquet européen. Les États membres qui participent à cette coopération renforcée devraient veiller à ce que le Parquet européen puisse, dans l'exercice de ses compétences prévues par les articles 22, 23 et 25 du règlement (UE) 2017/1939, solliciter une coopération en vertu du protocole au même titre que les procureurs nationaux de ces États membres. Ces instruments et accords concernent notamment les articles 8, 9, 10, 11 et 12 du protocole.

Par ailleurs, l'Union a adopté plusieurs directives qui renforcent les droits procéduraux des suspects et des personnes poursuivies[23]. Ces instruments concernent notamment les articles 6, 7, 8, 9, 10, 11, 12 et 13 du protocole. Un ensemble particulier de garanties touche à la protection des données à caractère personnel, qui constitue un droit fondamental consacré par les traités de l'UE et par la charte des droits fondamentaux de l'Union européenne. Les données à caractère personnel ne peuvent faire l'objet d'un traitement que dans le respect du règlement (UE) 2016/679 (règlement général sur la protection des données) et de la directive (UE) 2016/680 (directive en matière de protection des données dans le domaine répressif). Le droit fondamental de toute personne au respect de sa vie privée et familiale, de son domicile et de ses communications inclut le respect de la confidentialité de ses communications, en tant qu'élément essentiel de ce droit. Les données de communications électroniques ne peuvent faire l'objet d'un traitement que dans le respect de la

[23] 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); 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.

directive 2002/58/CE (directive «vie privée et communications»). Ces instruments concernent, en particulier, l'article 14 du protocole.

L'article 14 du protocole prévoit, en ses paragraphes 2 à 15, des garanties appropriées en matière de protection des données au sens, d'une part, des règles de l'Union dans ce domaine, en particulier l'article 46 du règlement général sur la protection des données et l'article 37 de la directive en matière de protection des données dans le domaine répressif, et, d'autre part, de la jurisprudence pertinente de la Cour de justice de l'Union européenne. Conformément aux exigences du droit de l'Union[24] et afin d'assurer l'effectivité des garanties énoncées à l'article 14 du protocole, les États membres devraient veiller à ce que les personnes dont les données ont été transférées en reçoivent notification, sous réserve de certaines restrictions, visant, par exemple, à éviter de compromettre des enquêtes en cours. L'article 14, paragraphe 11, point c), du protocole constitue la base juridique permettant aux États membres de satisfaire à cette exigence.

La compatibilité de l'article 14, paragraphe 1, du protocole avec les règles de l'Union en matière de protection des données impose également aux États membres d'examiner les points suivants en ce qui concerne d'autres possibilités de garantir la protection appropriée des données à caractère personnel transférées au titre du protocole. Pour ce qui est d'autres accords internationaux établissant un cadre global pour la protection des données à caractère personnel conformément aux exigences applicables de la législation des parties concernées, en application de l'article 14, paragraphe 1, point b), les États membres devraient prendre en compte la nécessité, aux fins d'une coopération directe, de compléter l'accord-cadre UE-États-Unis par des garanties supplémentaires – qui doivent être prévues dans un arrangement de transfert spécial entre les États-Unis et l'UE/ses États membres – intégrant les exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités[25].

De même, en application de l'article 14, paragraphe 1, point b), du protocole, les États membres ne devraient pas perdre de vue que, pour les États membres de l'UE qui sont parties à la convention 108+, cette dernière n'offre pas en soi une base appropriée pour les transferts de données transfrontières en vertu du protocole vers d'autres parties à cette convention. À cet

[24] Voir l'avis 1/15 de la Cour de justice (grande chambre), ECLI:EU:C:2017:592, point 220. Voir également la contribution du comité européen de la protection des données à la consultation sur un projet de deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest), 13 novembre 2019, p. 6 («Il importe que les autorités nationales compétentes auxquelles l'accès aux données a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. [L']information est nécessaire pour permettre à ces personnes d'exercer, notamment, leur droit de recours et leurs droits en matière de protection des données à l'égard du traitement de leurs données»).

[25] C'est pourquoi la décision du Conseil du 21 mai 2019 autorisant l'ouverture de négociations en vue de conclure un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale (9114/19) énonce, dans les directives de négociation, une série de garanties supplémentaires en matière de protection des données. En particulier, ces directives de négociation prévoient que «[l]'accord devrait compléter l'accord-cadre par des garanties supplémentaires tenant compte du niveau de sensibilité des catégories de données concernées et des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités et des transferts effectués directement par des autorités compétentes vers des fournisseurs de services».

égard, ils devraient prendre en compte l'article 14, paragraphe 1, dernière phrase, de la convention 108+[26].

Enfin, pour ce qui est des autres accords ou arrangements visés à l'article 14, paragraphe 1, point c), les États membres devraient tenir compte du fait qu'ils ne peuvent se prévaloir de ces autres accords ou arrangements que si la Commission européenne a adopté, au sujet du pays tiers concerné, une décision d'adéquation conformément à l'article 45 du règlement général (UE) 2016/679 sur la protection des données ou à l'article 36 de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif, décision qui s'applique aux transferts de données respectifs, ou si cet autre accord ou arrangement prévoit lui-même des garanties appropriées en matière de protection des données conformément à l'article 46 du règlement général sur la protection des données ou à l'article 37, paragraphe 1, point a), de la directive en matière de protection des données dans le domaine répressif.

Il convient de prendre en compte non seulement l'état actuel du droit de l'Union dans le domaine concerné, mais également ses perspectives d'évolution, dans la mesure où celles-ci sont prévisibles au moment de l'analyse. Le domaine couvert par le protocole présente un intérêt direct pour les perspectives d'évolution prévisibles du droit de l'Union. À cet égard, il conviendrait de mentionner les propositions de la Commission relatives à l'accès transfrontière aux preuves électroniques d'avril 2018[27]. Ces instruments concernent, en particulier, les articles 6 et 7 du protocole.

La Commission, tout en participant aux négociations au nom de l'Union, a veillé à ce que le protocole soit totalement compatible avec le droit de l'Union et les obligations qui incombent aux États membres en application de celui-ci. En particulier, la Commission a veillé à ce que les dispositions du protocole permettent aux États membres de respecter les droits fondamentaux, les libertés et les principes généraux du droit de l'Union, tels qu'inscrits dans les traités et la charte des droits fondamentaux de l'Union européenne, dont la proportionnalité, les droits procéduraux, la présomption d'innocence et les droits de la défense des personnes faisant l'objet d'une procédure pénale, ainsi que le respect de la vie privée, la protection des données à caractère personnel et des données de communications électroniques lorsqu'elles font l'objet d'un traitement, y compris les transferts aux services répressifs de pays non membres de l'Union européenne, et toute obligation qui incombe aux autorités répressives ou judiciaires à cet égard. La Commission a également pris en compte les avis respectifs du Contrôleur européen de la protection des données[28] et du comité européen de la protection des données[29].

---

[26] Voir également le rapport explicatif du protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 10 octobre 2018, points 106 et 107.

[27] COM(2018) 225 et 226 final.

[28] Avis 3/2019 du CEPD du 2 avril 2019 relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité.

[29] Notamment la «contribution du Comité européen de la protection des données à la consultation sur un projet de deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest) du 13 novembre 2019»; «Déclaration 02/201 relative au projet de dispositions nouvelles du deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest), adoptée le 2 février 2021»; «Contribution du comité européen de la protection des données du 4 mai 2021 au sixième cycle de consultations concernant le projet de deuxième protocole additionnel à la convention de Budapest du Conseil de l'Europe sur la cybercriminalité».

La Commission a en outre veillé à ce que les dispositions du protocole et les propositions de la Commission relatives aux preuves électroniques soient compatibles, notamment parce que ces projets d'actes législatifs ont évolué lors des discussions avec les colégislateurs, et à ce que le protocole ne donne pas lieu à des conflits de lois. En particulier, elle a veillé à ce que le protocole intègre des garanties appropriées en matière de protection des données et de la vie privée, ce qui permet aux fournisseurs de services de l'UE de se conformer aux obligations qui leur incombent en application de la législation de l'UE en matière de protection des données et de la vie privée, dans la mesure où le protocole sert de fondement juridique à des transferts de données à la suite d'injonctions ou de demandes émises par une autorité d'un État non membre de l'UE partie au protocole exigeant qu'un responsable du traitement ou un sous-traitant dans l'UE communique des données à caractère personnel ou des données de communications électroniques.

2.4. Réserves, déclarations, notifications et communications, et autres considérations

Le protocole fournit une base permettant aux parties de se prévaloir de certaines réserves et de faire des déclarations, des notifications ou des communications en ce qui concerne certains articles. Les États membres devraient adopter une approche uniforme de certaines réserves et déclarations, notifications et communications telles qu'énoncées en annexe de la présente décision. Afin que la mise en œuvre du protocole soit compatible avec le droit de l'Union, les États membres de l'UE devraient adopter la position exposée ci-après en ce qui concerne ces réserves et déclarations. Lorsque le protocole fournit une base pour d'autres réserves, déclarations, notifications ou communications, la présente proposition autorise les États membres à envisager leurs propres réserves, déclarations, notifications ou communications et à y procéder.

Afin de garantir la compatibilité entre les dispositions du protocole et le droit et les politiques de l'Union pertinents, les États membres ne devraient pas formuler les réserves prévues par l'article 7, paragraphe 9, point a)[30] et point b)[31]. Ils devraient en outre faire la déclaration prévue par l'article 7, paragraphe 2, point b)[32], et la notification prévue par l'article 7, paragraphe 5, point a)[33]. Il importe de ne pas formuler ces réserves et de soumettre la déclaration et la notification afin de garantir la compatibilité du protocole avec les propositions législatives de la Commission relatives aux preuves électroniques, en raison notamment de l'évolution de ces projets d'actes législatifs lors des discussions avec les colégislateurs.

---

[30] Autorisant les parties à se réserver le droit de ne pas appliquer l'article 7 (divulgation de données relatives aux abonnés).

[31] Autorisant les parties à se réserver le droit de ne pas appliquer l'article 7 (divulgation de données relatives aux abonnés) à certains types de numéros d'accès si cette divulgation était incompatible avec les principes fondamentaux de leur ordre juridique interne.

[32] Autorisant les parties à déclarer que l'injonction adressée en application de l'article 7, paragraphe 1 (divulgation de données relatives aux abonnés) doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante.

[33] Autorisant chaque partie à notifier au Secrétaire Général du Conseil de l'Europe qu'elle exige, lorsqu'une injonction est adressée en application de l'article 7, paragraphe 1 (divulgation de données relatives aux abonnés) à un fournisseur de services sur son territoire, dans chaque cas ou dans certaines circonstances déterminées, la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure.

En outre, afin d'assurer une application uniforme du protocole par les États membres de l'UE lorsqu'ils coopèrent avec des parties extérieures à l'UE, les États membres sont encouragés à ne pas se prévaloir de la réserve prévue par l'article 8, paragraphe 13[34], également parce qu'une telle réserve aurait un effet réciproque[35]. Les États membres devraient faire la déclaration prévue par l'article 8, paragraphe 4 afin de pouvoir donner effet à des injonctions au cas où des informations supplémentaires seraient nécessaires, concernant par exemple les circonstances de l'espèce afin d'apprécier la proportionnalité et la nécessité[36].

Les États membres sont également encouragés à s'abstenir de faire la déclaration prévue à l'article 9, paragraphe 1, point b)[37], afin d'assurer une application efficiente du protocole.

Les États membres devraient procéder aux communications prévues par l'article 7, paragraphe 5, point e)[38], par l'article 8, paragraphe 10, points a) et b)[39], par l'article 14, paragraphe 7, point c), et paragraphe 10, point b), afin d'assurer une application globalement efficace du protocole[40].

Enfin, les États membres devraient également prendre les mesures nécessaires conformément à l'article 14, paragraphe 11, point c), pour faire en sorte que la partie destinataire soit informée, au moment du transfert, de l'obligation imposée par le droit de l'Union de donner notification à la personne à laquelle les données se rapportent[41], et de fournir des coordonnées appropriées pour permettre à la partie destinataire d'informer l'autorité compétente de l'État membre de l'UE dès que les restrictions de confidentialité ne s'appliquent plus et que la notification peut être effectuée.

2.5. Motivation de la proposition

Le protocole entrera en vigueur après que cinq parties auront exprimé leur consentement à être liées par le protocole conformément aux dispositions de l'article 16, paragraphes 1 et 2 La cérémonie de signature du protocole devrait avoir lieu en mars 2022.

Il importe que les États membres de l'UE prennent les mesures nécessaires pour mettre en œuvre rapidement, et ce pour un certain nombre de raisons.

---

[34] Autorisant les parties à se réserver le droit de ne pas appliquer l'article 8 (donner effet aux injonctions d'une autre partie) aux données relatives au trafic.

[35] Voir le paragraphe 147 du rapport explicatif du protocole, selon lequel «[une] partie qui émet des réserves concernant cet article n'est pas autorisée à soumettre des injonctions de production de données relatives au trafic à d'autres parties en vertu [de l'article 8,] paragraphe 1».

[36] Autorisant les parties à déclarer que des informations supplémentaires sont nécessaires pour donner effet à des injonctions soumises en vertu de l'article 8, paragraphe 1 (donner effet aux injonctions d'une autre partie).

[37] Autorisant les parties à déclarer qu'elles n'exécuteront pas de demandes introduites en vertu de l'article 9, paragraphe 1, point a) (divulgation accélérée de données informatiques stockées, en cas d'urgence) pour la divulgation d'informations relatives à l'abonné seulement.

[38] Autorisant les parties à communiquer les coordonnées de l'autorité qu'elles désignent pour recevoir les notifications prévues à l'article 7, paragraphe 5, point a), et exécuter les tâches décrites à l'article 7, paragraphe 5, points b), c) et d) (divulgation de données relatives aux abonnés).

[39] Autorisant les parties à communiquer les coordonnées des autorités désignées pour soumettre et recevoir des injonctions en vertu de l'article 8 (donner effet aux injonctions d'une autre partie). Conformément aux exigences du règlement (UE) 2017/1939, les États membres qui participent à la coopération renforcée concernant la création du Parquet européen doivent inclure ce dernier dans la communication.

[40] Autorisant les parties à communiquer la ou les autorités qui devraient, respectivement, recevoir la notification en cas d'incident de sécurité, ou être contactée(s) pour solliciter l'autorisation préalable en cas de transferts ultérieurs vers un autre État ou vers une organisation internationale.

[41] Voir la note de bas de page 24 ci-dessus.

Premièrement, le protocole permettra d'améliorer les moyens dont disposent les autorités répressives et judiciaires pour obtenir les preuves électroniques dont elles ont besoin pour leurs enquêtes pénales Compte tenu de l'importance croissante des preuves électroniques pour les enquêtes pénales, il est, en effet, urgent de doter les autorités répressives et judiciaires des instruments appropriés pour obtenir un accès effectif à ces preuves afin qu'elles puissent lutter efficacement contre la criminalité en ligne.

Deuxièmement, le protocole garantira que les mesures visant à obtenir l'accès à des preuves électroniques sont mises en œuvre d'une manière qui permette aux États membres de respecter les droits fondamentaux, y compris les droits procéduraux en matière pénale, le droit au respect de la vie privée et le droit à la protection des données à caractère personnel En l'absence de règles claires au niveau international, les pratiques en vigueur peuvent être source de difficultés au regard de la sécurité juridique, de la transparence, de l'obligation de rendre des comptes ainsi que du respect des droits fondamentaux et des garanties procédurales des suspects dans les enquêtes pénales.

Troisièmement, le protocole permettra de résoudre et de prévenir les conflits de lois, qui touchent tant les autorités que les fournisseurs de services du secteur privé et d'autres entités, en prévoyant des règles compatibles au niveau international pour l'accès transfrontière aux preuves électroniques.

Quatrièmement, le protocole confirmera l'importance que continue de revêtir la convention en tant que principal cadre multilatéral de lutte contre la cybercriminalité. Cela sera essentiel pour le processus consécutif à la résolution 74/247 de l'Assemblée générale des Nations unies (AGNU) de décembre 2019 sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, qui a institué un comité intergouvernemental spécial d'experts à composition non limitée 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.

3. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- *Base juridique*

La compétence de l'Union pour légiférer sur des questions visant à faciliter la coopération entre autorités judiciaires ou équivalentes dans le cadre des procédures pénales et de l'exécution des décisions est fondée sur l'article 82, paragraphe 1, du TFUE. La compétence de l'Union en matière de protection des données à caractère personnel est fondée sur l'article 16 du TFUE.

Conformément à l'article 3, paragraphe 2, du TFUE, 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 de l'UE ou d'en altérer la portée. Les dispositions du protocole relèvent d'un domaine couvert dans une large mesure par des règles communes, comme indiqué au point 2.3 ci-dessus.

Le protocole relève donc de la compétence externe exclusive de l'Union. Les États membres peuvent donc signer le protocole, dans l'intérêt de l'Union, sur la base de l'article 16, de l'article 82, paragraphe 1, et de l'article 218, paragraphe 5, du TFUE.

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

Sans objet.

- *Proportionnalité*

En ce qui concerne la présente proposition, les objectifs de l'Union, tels qu'ils sont énoncés au point 2.5 ci-dessus, ne peuvent être atteints que par la conclusion d'un accord international contraignant prévoyant les mesures de coopération nécessaires tout en assurant une protection appropriée des droits fondamentaux. Le protocole réalise cet objectif. Les dispositions du protocole sont limitées à ce qui est nécessaire pour atteindre ses principaux objectifs. Une action unilatérale ne constitue pas une alternative car elle n'offre pas une base suffisante de coopération avec les pays tiers et ne permettrait pas d'assurer la protection nécessaire des droits fondamentaux. En outre, l'adhésion à un accord multilatéral tel que le protocole, que l'Union a pu négocier, est plus efficace que l'ouverture de négociations bilatérales avec différents pays tiers. En partant du principe de sa ratification par les 66 parties, ainsi que par les futures nouvelles parties, à la convention, le protocole offrira un cadre juridique commun pour la coopération des États membres de l'UE avec leurs partenaires internationaux les plus importants en matière de lutte contre la criminalité.

- ***Choix de l'instrument***

Sans objet.

4. 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 Conseil de l'Europe a organisé six cycles de consultations publiques concernant les négociations sur le protocole, en juillet et novembre 2018, février et novembre 2019, décembre 2020 et mai 2021[42]. Les parties ont tenu compte des contributions reçues dans le cadre de ces consultations.

La Commission, en tant que négociatrice au nom de l'Union, a également procédé à des échanges de vues avec les autorités chargées de la protection des données et a organisé des réunions de consultation ciblées tout au long de 2019 et 2021 avec des organisations de la société civile, des fournisseurs de services et des associations professionnelles. Elle a tenu compte des contributions reçues lors de ces échanges.

- *Obtention et utilisation d'expertise*

Au cours des négociations, la Commission a systématiquement consulté le comité spécial du Conseil pour les négociations, conformément à la décision du Conseil de l'Union européenne du 6 juin 2019 autorisant la Commission à participer, au nom de l'Union, aux négociations, ce qui a permis aux experts des États membres de contribuer au processus d'élaboration de la position de l'Union. Plusieurs experts des États membres ont également continué à participer aux négociations, parallèlement à la participation de la Commission au nom de l'Union. Les parties prenantes ont également été consultées (voir ci-dessus).

[42] https://www.coe.int/fr/web/cybercrime/protocol-consultations

- *Analyse d'impact*

Une analyse d'impact a été réalisée en 2017-2018 pour accompagner les propositions de la Commission concernant les preuves électroniques[43]. Dans ce contexte, la négociation d'un accord sur un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité a constitué un volet de l'option retenue. Les incidences pertinentes sont en outre développées dans le présent exposé des motifs.

- *Réglementation affûtée et simplification*

Le protocole peut avoir une incidence sur certaines catégories de fournisseurs de services, y compris les petites et moyennes entreprises (PME), étant donné que ceux-ci peuvent faire l'objet de demandes et d'injonctions relatives à des preuves électroniques en application du protocole. Toutefois, ces fournisseurs de services reçoivent déjà souvent des demandes de ce type par l'intermédiaire d'autres canaux existants, qui sont parfois transmises par d'autres autorités, notamment sur le fondement de la convention[44], d'autres traités d'entraide judiciaire ou d'autres cadres, y compris les politiques multipartites en matière de gouvernance de l'internet[45]. En outre, les fournisseurs de services, dont les PME, profiteront d'un cadre juridique clair au niveau international et d'une approche commune de toutes les parties au protocole.

- *Droits fondamentaux*

Lorsque les données d'une personne peuvent être obtenues dans le cadre d'une procédure pénale, les instruments de coopération prévus par le protocole sont susceptibles de porter atteinte aux droits fondamentaux, y compris le droit à accéder à un tribunal impartial, le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. Le protocole suit une approche fondée sur les droits et prévoit des conditions et des garanties conformes aux instruments internationaux relatifs aux droits de l'homme, parmi lesquels la convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe de 1950. Le protocole prévoit notamment des garanties spécifiques en matière de protection des données. En tant que de besoin, il constitue également une base juridique permettant aux parties de faire certaines réserves, déclarations ou notifications, et prévoit des motifs pour lesquels une coopération peut être refusée dans des situations particulières. La compatibilité du protocole avec la charte des droits fondamentaux de l'Union européenne est ainsi garantie.

5. INCIDENCE BUDGÉTAIRE

La proposition n'a pas d'incidence sur le budget de l'Union. La mise en œuvre du protocole peut engendrer des coûts ponctuels pour les États membres et l'augmentation attendue du nombre d'affaires pourrait faire supporter des coûts plus élevés à leurs autorités.

---

43 SWD(2018) 118 final.

44 Voir, par exemple, la note d'orientation T-CY #10 du Comité de la Convention sur la cybercriminalité du 1er mars 2017 sur les injonctions de production concernant des informations sur les abonnés (article 18 de la convention de Budapest).

45 Voir, par exemple, la résolution du conseil d'administration de la société pour l'attribution des noms de domaine et des numéros sur internet (ICANN) du 15 mai 2019 sur les recommandations concernant la spécification temporaire relative aux données d'enregistrement des gTLD, disponible à l'adresse suivante: www.icann.org.

6. 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 le protocole après sa signature et sa ratification, il n'existe pas de plan de mise en œuvre.

En ce qui concerne le suivi, la Commission prendra part aux réunions du Comité de la Convention sur la cybercriminalité, au sein duquel l'Union européenne est reconnue comme une organisation ayant le statut d'observateur.

2021/0382 (NLE)

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

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 et son article 218, paragraphe 5,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Le 9 juin 2019, le Conseil a autorisé la Commission à participer, au nom de l'Union européenne, aux négociations relatives au deuxième protocole additionnel à la convention de Budapest du Conseil de l'Europe sur la cybercriminalité.

(2) Le texte du deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (ci-après le «protocole») a été adopté par le Comité des ministres du Conseil de l'Europe le 17 novembre 2021 et devrait être ouvert à la signature en mars 2022.

(3) Les dispositions du protocole relèvent d'un domaine couvert dans une large mesure par des règles communes au sens de l'article 3, paragraphe 2, du TFUE, y compris par des instruments facilitant la coopération judiciaire en matière pénale, garantissant des normes minimales pour les droits procéduraux, et prévoyant des garanties en matière de protection des données et de la vie privée.

(4) La Commission a également présenté une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale [COM(2018) 225 final], ainsi qu'une 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], qui instaurent des injonctions européennes transfrontières contraignantes de production et de conservation devant être adressées directement à un représentant d'un fournisseur de services dans un autre État membre.

(5) En participant aux négociations, au nom de l'Union, la Commission a veillé à la compatibilité du deuxième protocole additionnel avec les règles communes pertinentes de l'Union européenne.

(6) Un certain nombre de réserves, déclarations, notifications et communications sont pertinentes pour garantir la compatibilité du protocole avec le droit et les politiques de l'Union, l'application uniforme du protocole entre les États membres de l'UE dans

leurs relations avec les parties non membres de l'UE, ainsi que l'application effective du protocole.

(7) Dans la mesure où le protocole prévoit des procédures rapides qui améliorent l'accès transfrontière à des preuves électroniques et un niveau élevé de garanties, son entrée en vigueur contribuera à la lutte contre la cybercriminalité et d'autres formes de criminalité au niveau mondial en facilitant la coopération entre les parties au protocole qui sont des États membres de l'UE et celles qui ne le sont pas, permettra d'assurer un niveau élevé de protection des personnes et de résoudre les conflits de lois.

(8) Étant donné que le protocole prévoit des garanties appropriées conformes aux exigences applicables aux transferts internationaux de données à caractère personnel au titre du règlement (UE) 2016/679 et de la directive (UE) 2016/680, son entrée en vigueur contribuera à promouvoir les normes de l'Union en matière de protection des données au niveau mondial, facilitera les flux de données entre les parties au protocole qui sont des États membres de l'UE et celles qui ne le sont pas et garantira le respect, par les États membres de l'UE, des obligations qui leur incombent en application des règles de l'Union relatives à la protection des données.

(9) L'entrée en vigueur rapide consolidera également le rôle de la convention de Budapest du Conseil de l'Europe en tant que principal cadre multilatéral de lutte contre la cybercriminalité.

(10) L'Union européenne ne peut être partie au protocole, étant donné que tant le protocole que la convention du Conseil de l'Europe sur la cybercriminalité sont ouverts aux seuls États.

(11) Il convient donc d'autoriser les États membres, agissant conjointement dans l'intérêt de l'Union européenne, à signer le protocole.

(12) Les États membres sont encouragés à signer le protocole pendant la cérémonie de signature, ou dans les meilleurs délais après celle-ci.

(13) 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 ....

(14) [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].

[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 a notifié [, par lettre du ...,] son souhait de participer à l'adoption et à l'application de la présente décision].

(15) Conformément aux articles 1er et 2 du protocole nº 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

Les États membres sont autorisés 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 (ci-après le «protocole»).

Article 2

Lors de la signature du protocole, les États membres font les réserves, déclarations, communications ou notifications qui figurent en annexe.

Article 3

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

Article 4

La présente décision est publiée au *Journal officiel de l'Union européenne*.

Article 5

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le

Par le Conseil
Le président