

Procedure file

Informations de base		
NLE - Procédures non législatives	2021/0383(NLE)	En attente de décision finale
Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques: deuxième protocole additionnel Voir aussi 2022/2967(RSP)		
Sujet 3.30.07 Cybersécurité, politique cyberspace 3.30.25 Réseaux mondiaux et société de l'information, internet		

Acteurs principaux			
Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	LIBE Libertés civiles, justice et affaires intérieures	 LÓPEZ AGUILAR Juan Fernando Rapporteur(e) fictif/fictive  BRAUNSBERGER-REINHOLD Karolin  KÖRNER Moritz  LAGODINSKY Sergey  TARDINO Annalisa  KANKO Assita	
Conseil de l'Union européenne Commission européenne	DG de la Commission Migration et affaires intérieures	Commissaire JOHANSSON Ylva	

Evénements clés			
25/11/2021	Document préparatoire	COM(2021)0719	
06/04/2022	Publication de la proposition législative	06438/2022	Résumé
07/04/2022	Annonce en plénière de la saisine de la commission		

12/01/2023	Vote en commission		
13/01/2023	Dépôt du rapport de la commission, 1ère lecture/lecture unique	A9-0002/2023	
17/01/2023	Résultat du vote au parlement		
17/01/2023	Décision du Parlement	T9-0002/2023	Résumé

Informations techniques

Référence de procédure	2021/0383(NLE)
Type de procédure	NLE - Procédures non législatives
Sous-type de procédure	Approbation du Parlement
	Voir aussi 2022/2967(RSP)
Etape de la procédure	En attente de décision finale
Dossier de la commission parlementaire	LIBE/9/07837

Portail de documentation

Document annexé à la procédure	COM(2021)0718	25/11/2021	EC	
Document préparatoire	COM(2021)0719	25/11/2021	EC	
Document annexé à la procédure	N9-0021/2022 JO C 182 04.05.2022, p. 0015	20/01/2022	EDPS	
Document de base législatif	06438/2022	06/04/2022	CSL	Résumé
Projet de rapport de la commission	PE740.540	21/12/2022	EP	
Amendements déposés en commission	PE740.618	10/01/2023	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique	A9-0002/2023	13/01/2023	EP	
Texte adopté du Parlement, 1ère lecture/lecture unique	T9-0002/2023	17/01/2023	EP	Résumé

Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques: deuxième protocole additionnel

OBJECTIF : autoriser 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.

ACTE PROPOSÉ : Décision du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Conseil ne peut adopter l'acte que si le Parlement européen a approuvé celui-ci.

CONTEXTE : la cybercriminalité continue de représenter un défi considérable. 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 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.

Le 6 juin 2019, le Conseil a autorisé la Commission à participer, au nom de l'Union, aux négociations relatives au deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (STCE n° 185) (convention sur la cybercriminalité).

La convention de Budapest sur la cybercriminalité a pour objectif de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques. La convention :

- contient des dispositions harmonisant les éléments constitutifs des infractions en droit pénal matériel national et des dispositions connexes dans le domaine de la cybercriminalité,
- prévoit les pouvoirs nécessaires en 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

- vise à mettre en place un système rapide et efficace de coopération internationale.

La Commission s'est engagée à assurer une conclusion rapide des négociations sur le protocole. En participant aux négociations sur le protocole, la Commission a veillé à sa compatibilité avec les règles communes pertinentes de l'Union. 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.

Le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques a été adopté par le Comité des ministres du Conseil de l'Europe le 17 novembre 2021 et devrait être ouvert à la signature le 12 mai 2022.

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 traité sur le fonctionnement de l'Union européenne (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.

CONTENU : le projet de décision du Conseil vise à autoriser les États membres à ratifier, dans l'intérêt de l'Union, le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

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.

Le protocole :

- 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;
- détermine les langues dans lesquelles les parties doivent présenter les injonctions, les demandes ou les notifications au titre du protocole;
- prévoit que les parties assurent la coopération mutuelle la plus large possible et 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 en facilitant la coopération entre les États membres parties au protocole et les pays tiers parties au protocole, permettra d'assurer un niveau élevé de protection des personnes et résoudra les conflits de lois.

Le Protocole offre une base :

- pour la coopération directe entre les autorités compétentes sur le territoire d'une partie et les entités fournissant des services de registre 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;
- 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;
- en vue du renforcement de la coopération entre autorités pour la divulgation de données informatiques;
- en vue de la coopération entre autorités pour la divulgation de données informatiques en situation d'urgence;
- pour l'entraide judiciaire en situation d'urgence;
- pour la coopération par vidéoconférence;
- pour les enquêtes communes et les équipes communes d'enquête.

L'entrée en vigueur du protocole contribuera à promouvoir les normes de l'Union en matière de protection des données au niveau mondial, facilitera les flux de données entre les États membres parties au protocole et les pays tiers parties au protocole et garantira le respect, par les États membres parties au protocole, des obligations qui leur incombent en application des règles de l'Union relatives à la protection des données.

Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques: deuxième protocole additionnel

Le Parlement européen a adopté par 436 voix pour, 168 contre et 35 abstentions, une résolution législative sur le projet de décision du Conseil autorisant les États membres à ratifier, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

Suivant la recommandation de la commission des libertés civiles, de la justice et des affaires intérieures, le Parlement a donné son approbation au projet de décision du Conseil.

Le projet de décision du Conseil vise à autoriser les États membres à ratifier, dans l'intérêt de l'Union, le deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

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 l'Europe de 1950.

Le protocole prévoit également des garanties solides pour la protection de la vie privée et des données à caractère personnel.

Transparence			
SIPPEL Birgit	Membre	11/01/2023	Council of Europe