Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Avis 299 (2021)[1]

Projet de deuxième protocole additionnel à la Convention sur la cybercriminalité (STE n° 185) relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Assemblée parlementaire

1. L'Assemblée parlementaire rappelle que le 20e anniversaire de l'adoption de la Convention sur la cybercriminalité (STE no 185) sera célébré en novembre 2021. Elle se félicite du succès rencontré dans le monde par cette convention du Conseil de l'Europe, qui compte à l'heure actuelle 66 ratifications.

2. L'Assemblée observe que, depuis 2001, l'exploitation des technologies de l'information à des fins criminelles a fortement augmenté. De nombreux États considèrent la cybercriminalité comme une grave menace pour les droits de l'homme, l'État de droit et le fonctionnement des sociétés démocratiques, voire pour la sécurité nationale. Parmi les exemples de cybercriminalité figurent les violences sexuelles en ligne sur mineur, le vol et l'utilisation détournée de données personnelles, l'ingérence dans les processus électoraux et autres attaques contre des institutions démocratiques, les attaques contre des infrastructures étatiques et de service public essentielles, l'utilisation abusive de ces technologies à des fins terroristes et, pendant l'actuelle pandémie de covid-19, les cyberattaques contre les hôpitaux et les laboratoires qui développent des vaccins contre le virus, et l'usurpation de noms de domaine à des fins de promotion de faux vaccins et traitements.

3. Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité vise à fournir des outils plus puissants pour enquêter en la matière ainsi qu'à rendre justice aux victimes. Eu égard à l'ampleur actuelle de la cybercriminalité, il importe d'améliorer les chances des victimes de violence en ligne d'obtenir justice et d'alourdir considérablement le risque, pour les auteurs de ces infractions, d'avoir à répondre de leurs actes.

4. L'Assemblée rappelle ses précédents travaux sur la lutte contre la cybercriminalité, notamment son Avis 226 (2001) «Projet de convention sur la cybercriminalité», son Avis 240 (2002) «Projet de protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques», ses Recommandations 2041 (2014) **«**Améliorer la protection et la sécurité des utilisateurs dans le cyberespace» et 2077 (2015) «Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet», et, plus récemment, sa Résolution 2256 (2019) «Gouvernance de l'internet et droits de l'homme». L'Assemblée a constamment adopté une approche constructive pour améliorer la coopération internationale dans ce domaine, tout en protégeant les droits de l'homme.

5. L'Assemblée reconnaît que le projet de deuxième protocole additionnel est conçu pour fonctionner au sein des systèmes de justice pénale des Parties, assorti de l'ensemble des procédures, réglementations, méthodes de transmission des données, conditions et garanties prévues par leurs ordres juridiques internes respectifs. Cela vaut également pour la «coopération directe» prévue aux articles 6 et 7, qui imposent tous deux aux Parties d'établir un fondement juridique interne satisfaisant pour l'exercice de ces compétences.

6. L'Assemblée reconnaît par ailleurs qu'il existe un dilemme difficile concernant à la fois la Convention sur la cybercriminalité elle-même et ses protocoles additionnels. Le but poursuivi par ces traités présuppose que le plus grand nombre possible d'États participent à la lutte contre la cybercriminalité, car cette dernière ne

1. *Discussion par l'Assemblée* le 30 septembre 2021 (30e séance) (voir Doc. 15379 et Doc. 15379, rapport de la commission des questions juridiques et des droits de l'homme, rapporteur: M. Kamal Jafarov). *Texte adopté par l'Assemblée* le 30 septembre 2021 (30e séance).

reconnaît aucune frontière. S'ils ne le font pas, les cybercriminels continueront à agir depuis des sanctuaires préservés, au détriment de leurs victimes dans le monde entier. Les ordres juridiques varient considérablement d'un pays à l'autre, y compris dans le domaine du droit pénal et des différents niveaux de réglementation de la protection des données. La convention et ses protocoles peuvent par conséquent établir uniquement des normes minimales de protection, qui doivent être mises en œuvre par l'ensemble des États participants, tout en laissant aux États plus avancés la possibilité de prévoir des protections renforcées au profit de leurs citoyens. Cependant, ces normes plus rigoureuses de protection ne doivent pas compromettre l'objectif commun de la convention et de ses protocoles, à savoir renforcer l'efficacité et l'effectivité de la coopération internationale dans la lutte contre la cybercriminalité.

7. L'Assemblée estime que le projet de deuxième protocole additionnel à la Convention sur la cybercriminalité ménage en principe un équilibre raisonnable face au dilemme précité. Ayant examiné les nombreuses propositions faites par les différentes parties prenantes, elle propose néanmoins d'apporter les améliorations suivantes pour renforcer davantage la protection des droits humains, en particulier le droit au respect de la vie privée:

7.1. consacrer l'application du principe de proportionnalité dans le texte de l'article 13, en plus de sa mention dans le rapport explicatif du projet de protocole;

7.2. préciser, à l'article 14, paragraphe 2, que le traitement ultérieur des données à caractère personnel par la Partie destinataire doit être prévu par la loi et constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir d'importants objectifs d'intérêt public général ou, à défaut, prévoir une protection satisfaisante des droits humains et des libertés;

7.3. ajouter à la liste des informations mises à la disposition des personnes concernées prévues à l'article 14, paragraphe 11, les coordonnées du ou de la responsable du traitement compétente;

7.4. revoir le paragraphe 12.*b* du projet de protocole, en indiquant qu'en règle générale les informations relatives à l'accès et à la rectification sont fournies gratuitement aux personnes concernées;

7.5. reconnaître expressément dans le texte du projet de protocole ou de son rapport explicatif que les privilèges et immunités de certaines professions, comme les avocats, les médecins, les journalistes, les ministres du culte ou les parlementaires, doivent être respectés;

7.6. rendre obligatoire la communication publique, par les autorités de surveillance, des données agrégées sur l'emploi des mesures prévues par le protocole et sur le nombre de personnes touchées par ces mesures;

7.7. mentionner les mesures de protection des témoins existant au niveau national dans les dispositions autorisant l'obtention de preuves par vidéoconférence, et prévoir la possibilité pour l'avocat de participer à l'audition en vidéoconférence pour défendre les intérêts de son client ou de sa cliente;

7.8. renforcer «l'égalité des armes» entre le ministère public et la défense, en obligeant les autorités compétentes des Parties à faire usage des instruments d'enquête mis à leur disposition par le projet de protocole également pour le compte de la défense.