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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15379
27 septembre 2021

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

Rapport[1]
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Kamal JAFAROV, Azerbaïdjan, Groupe des Conservateurs européens et Alliance démocratique

Résumé

La commission des questions juridiques et des droits de l'homme se félicite du succès que rencontre la Convention sur la cybercriminalité (STE n° 185) dans le monde, avec 66 ratifications. Elle note que depuis l'adoption de la Convention en 2001, l'exploitation des technologies de l'information à des fins criminelles a fortement augmenté. La cybercriminalité est considérée par de nombreux États comme une menace grave pour les droits de l'homme, l'État de droit et le fonctionnement des sociétés démocratiques, voire pour la sécurité nationale.

L'objectif du Deuxième Protocole additionnel à la Convention sur la cybercriminalité est de fournir des outils plus pointus pour enquêter sur la cybercriminalité et obtenir justice pour les victimes. Le projet de Protocole est conçu pour fonctionner dans le cadre des systèmes de justice pénale des Parties avec toutes les procédures, réglementations, méthodes de transmission des données, conditions et garanties prévues dans les systèmes juridiques nationaux respectifs.

La Convention sur la cybercriminalité et ses Protocoles additionnels sont confrontés à un dilemme. L'objectif de ces traités présuppose que le plus grand nombre possible d'États participent à la lutte contre la cybercriminalité, celle-ci ne connaissant pas de frontières. Or, les systèmes juridiques des États diffèrent, y compris dans les domaines du droit pénal et de la protection des données. La Convention et ses Protocoles ne peuvent donc que fixer des normes minimales de protection qui doivent être mises en œuvre par tous les États participants, tout en laissant la possibilité aux États plus avancés de mettre en œuvre des protections plus fortes. Mais ces protections plus développées ne doivent pas compromettre l'objectif commun de la Convention et de ses Protocoles, à savoir rendre la coopération internationale dans la lutte contre la cybercriminalité plus efficace.

La commission considère que le Deuxième Protocole additionnel établit en principe un équilibre raisonnable. Ayant examiné de nombreuses propositions émanant de différentes parties prenantes, elle suggère néanmoins quelques améliorations pour renforcer davantage la protection des droits humains.

1. Renvoi en commission: Doc. 15316, Renvoi 4593 du 21 juin 2021.

Sommaire **Page**

A. Projet d'avis 3
B. Exposé des motifs par M. Kamal Jafarov, rapporteur 5
1. Contexte 5
2. Travaux antérieurs de l'Assemblée 5
3. Principales caractéristiques du projet de Deuxième Protocole additionnel 7
4. Critiques et recommandations émanant de parties prenantes 7
5. Évaluation des commentaires et propositions 11
6. Conclusions 17
Annexe - Audition du 14 septembre 2021 18

A. Projet d'avis[2]

1. L'Assemblée parlementaire rappelle que le 20e anniversaire de l'adoption de la Convention sur la cybercriminalité (STE n° 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 sur mineur en ligne, 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 la 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, notamment.

3. Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité vise à améliorer les outils d'enquête en la matière et à rendre justice aux victimes. Eu égard à l'ampleur actuelle de la cybercriminalité, il importe d'améliorer les chances des victimes 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 des 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 Protocole 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 par les 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 que la Convention sur la cybercriminalité et ses Protocoles additionnels sont confrontés à un dilemme difficile. 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 reconnaît aucune frontière. Dans le cas contraire, 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. Mais 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 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;

2. Projet d'avis adopté à l'unanimité par la commission le 27 septembre 2021.

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. actualiser le paragraphe 12.b, 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, médecins, journalistes, ministres du culte ou 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 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.

B. Exposé des motifs par M. Kamal Jafarov, rapporteur

1. Contexte

1. La Convention sur la cybercriminalité (STE n° 185, également connue sous le nom de « Convention de Budapest » ou «Convention Cybercriminalité»), ouverte à la signature en 2001, rassemble des Parties de toutes les régions du monde (66 ratifications en juin 2021). Les États-Unis d'Amérique sont Partie à la Convention elle-même, mais pas à son (premier) Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189). Ce point avait été omis dans la Convention Cybercriminalité pour que les États-Unis puissent la signer malgré la protection étendue de la liberté d'expression que prévoit leur Constitution. La Fédération de Russie est le seul État membre du Conseil de l'Europe à n'avoir ni signé ni ratifié la Convention Cybercriminalité; l'Irlande l'a signée, mais pas ratifiée.

2. L'utilisation des technologies de l'information à des fins criminelles a pris un essor considérable depuis 2001. La cybercriminalité est vue par de nombreux États comme une grave menace pesant sur les droits humains, l'État de droit et le fonctionnement des sociétés démocratiques, voire sur la sécurité nationale. Le rapport explicatif du projet de Deuxième Protocole additionnel en donne de nombreux exemples, notamment la violence sexuelle exercée en ligne contre des enfants, le vol et l'utilisation détournée de données personnelles («usurpation d'identité»), l'ingérence dans des processus électoraux et autres attaques contre des institutions démocratiques, les attaques contre des infrastructures essentielles (par exemple par «déni de service» ou «logiciel rançonneur»), ou l'utilisation détournée de ces technologies à des fins terroristes. Pendant la pandémie de covid-19, les pays en ont observé des formes variées: attaques contre les hôpitaux et établissements médicaux qui développent des vaccins contre le virus, usurpation de noms de domaine à des fins de promotion de faux vaccins et traitements, par exemple.

3. La Convention Cybercriminalité et ses Protocoles additionnels, dont le deuxième, objet du présent avis[3], sont confrontés à un dilemme difficile. Pour atteindre leurs buts, ils doivent rassembler le plus grand nombre possible d'États, la cybercriminalité ignorant les frontières, faute de quoi les cybercriminels continueront à opérer depuis des lieux sûrs, et à faire des victimes dans le reste du monde. Or les systèmes juridiques diffèrent énormément d'un pays à l'autre, y compris en matière pénale, et force est d'admettre que l'on y observe des degrés variables de sensibilisation à la protection des données et de réglementation en la matière. La Convention et ses Protocoles ne peuvent donc fixer que des règles de protection minimale, qui seront impérativement appliquées dans tous les États Parties, et laisser les États plus avancés ériger une protection plus solide pour leurs populations respectives. Mais ces normes plus strictes ne doivent pas compromettre l'objectif commun de la Convention et de ses Protocoles, en particulier le projet de Deuxième Protocole additionnel, à savoir donner plus d'efficacité et d'efficience à la coopération internationale dans la lutte contre la cybercriminalité. Selon moi, les rédacteurs du Deuxième Protocole additionnel sont parvenus en principe à ménager un juste équilibre entre les intérêts en présence, face au dilemme susmentionné. Après avoir examiné les nombreuses propositions formulées par les différentes parties prenantes, je propose néanmoins quelques modifications à apporter au projet de Protocole, en vue de renforcer la protection des droits de l'homme, et plus particulièrement le droit au respect de la vie privée (voir plus loin le chapitre 5).

2. Travaux antérieurs de l'Assemblée

4. Les travaux antérieurs de l'Assemblée montrent qu'elle a toujours été favorable à une action ferme de lutte contre la cybercriminalité tout en préconisant le plus haut niveau possible de protection du droit à la vie privée des utilisateurs d'internet.

5. Dans son Avis no 226 (2001) «Projet de convention sur la cybercriminalité», l'Assemblée considérait que la lutte contre la criminalité cybernétique constitue un enjeu de toute première importance au regard des obstacles que peut poser cette forme de criminalité au développement des nouvelles technologies. (paragraphe 1) et notait qu'il est essentiel que des définitions communes des crimes soient établies ; que le secteur privé continue de travailler à la sécurisation informatique des réseaux ; et que les gouvernements édictent des lois nationales adaptées et proportionnées (paragraphe 4). Dans les nombreuses modifications qu'elle proposait, elle insistait sur la nécessité de mieux protéger le droit à la vie privée et de négocier promptement un Protocole additionnel élargissant le champ d'application à « de nouvelles formes d'infraction » comme «la diffusion de propagande raciste, l'hébergement abusif de communications haineuses, l'utilisation d'Internet aux fins de trafic d'êtres humains et l'entrave au fonctionnement du système

3. Voir Doc. 15316rev.

informatique au moyen des *spam* (courriers-poubelles)». Dans son exposé des motifs, le rapporteur formulait son « refus absolu d'une 'cyberpolice' transcendant les frontières et les souverainetés nationales. Il s'entend qu'une "cyberpolice" qui dépasserait le cadre des États et de leurs compétences souveraines devrait être exclue. […] Ainsi, un État peut effectuer une enquête pour le compte d'un autre, mais ne peut mener d'enquêtes ni de perquisitions transfrontalières. Contrairement aux craintes exprimées, les téléperquisitions ne seraient par conséquent pas prévues par le projet de convention. Cette position est en opposition avec celle des États-Unis, qui estiment que les enquêteurs spécialisés dans Internet doivent disposer de libertés en rapport avec le caractère international du réseau des réseaux. » La suite a montré que les outils créés par la Convention ne suffisaient pas, eu égard à la flambée de la cybercriminalité — ce qui a conduit à la négociation du Deuxième Protocole additionnel.

6. Dans son Avis 240 (2002) «Projet de protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques», l'Assemblée « reconnaît que le texte adopté par le Comité européen pour les problèmes criminels est un compromis entre des traditions juridiques et culturelles différentes, compromis qui lui donne en grande partie satisfaction dans l'équilibre trouvé entre le combat contre le racisme et la liberté d'expression » (paragraphe 4). La principale modification qu'elle proposait (l'introduction de la notion «d'hébergement abusif») n'a pas été retenue dans la dernière version du projet.

7. Dans sa Recommandation 2041 (2014) « Améliorer la protection et la sécurité des utilisateurs dans le cyberespace », l'Assemblée invitait le Comité des Ministres à examiner la possibilité d'élaborer un Protocole additionnel à la Convention sur la cybercriminalité concernant les violations graves des droits fondamentaux des utilisateurs de services en ligne, et de déterminer dans quelle mesure la Convention européenne sur l'entraide judiciaire en matière pénale (STE n° 30) devait être actualisée afin de couvrir l'entraide dans les affaires de cybercriminalité transnationale ainsi que les cyberpreuves. Elle invitait aussi le Comité des Ministres à établir, sur la base des éléments divulgués par Edward Snowden concernant les violations massives du droit à la vie privée, consacré par l'article 8 de la Convention européenne des droits de l'homme (STE N° 5), un plan d'action visant à prévenir pareilles violations (paragraphes 2.1, 2.2 et 2.9).

8. Dans sa Recommandation 2077 (2015) « Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur Internet », l'Assemblée recommandait au Comité des Ministres d'inviter les Parties à la Convention sur la cybercriminalité et à son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques à étudier s'il était faisable «d'élaborer un protocole additionnel définissant un niveau commun d'incrimination des cyberattaques de grande ampleur […], ainsi que sur des normes minimales pour les peines applicables à ces attaques ; d'élaborer un autre protocole additionnel sur l'entraide en matière de pouvoirs d'investigation, qui étende en particulier le champ d'application de l'article 32 de la convention […] ; et d'étudier la faisabilité d'un «protocole additionnel à la Convention sur la cybercriminalité relatif à l'accès de la justice pénale aux données stockées sur des serveurs d'hébergement dans le nuage». Elle lui demandait en outre «d'élaborer des normes juridiques sur la responsabilité internationale qui revient aux États de prendre toutes les mesures raisonnables pour prévenir que des cyberattaques de grande ampleur soient lancées par des personnes relevant de leur juridiction ou à partir de leur territoire national contre des systèmes informatiques dans un autre État.» (Paragraphes 3.1. à 3.3.).

9. Plus récemment, dans sa Résolution 2256 (2019) « Gouvernance de l'Internet et droits de l'homme », l'Assemblée réaffirmait la nécessité de mieux protéger les droits humains sur internet. Tout en soulignant la nécessité de garantir la protection effective du droit à la liberté d'expression et d'information en ligne et hors ligne, elle notait qu'il convenait de faire plus pour contrer les dangers qu'engendrent les abus de ces droits, tels que l'incitation à la discrimination, à la haine et à la violence, dont le terrorisme, l'abus sexuel d'enfants, le cyberharcèlement, la manipulation de l'information et la propagande. Cette exigence se double de la nécessité de garantir qu'internet devienne un environnement sécurisé, où les usagers sont à l'abri de l'arbitraire, des menaces, des atteintes à l'intégrité physique et psychique, et des violations de leurs droits. L'Assemblée soulignait à nouveau la menace que représentent pour les droits humains les systèmes d'envergure mis en place par les services de renseignement en vue de collecter, de conserver et d'analyser à grande échelle les données des communications. Elle recommandait ainsi aux États membres du Conseil de l'Europe « de réfléchir à des politiques globales de lutte contre la criminalité informatique […] y compris l'établissement de forces de police spécialisées dans le dépistage et l'identification des criminels informatiques, et dotées de moyens techniques adéquats […]» (paragraphes 5-7, 9.3). L'Assemblée considérait que la Convention sur la cybercriminalité devait être mieux utilisée pour améliorer la collaboration interétatique; elle appelait les États membres à la ratifier s'ils ne l'avaient pas encore fait, et à encourager l'achèvement des négociations sur le Deuxième Protocole additionnel sur une coopération internationale renforcée et l'accès aux preuves d'activités criminelles stockées dans le nuage (paragraphe 11).

3. Principales caractéristiques du projet de Deuxième Protocole additionnel

10. Le **chapitre II** du projet de Deuxième Protocole («le projet de Protocole» ou «le Protocole») prévoit des « mesures de coopération renforcée », dont, à la **section 2**, des « procédures renforçant la coopération directe avec les fournisseurs et les entités dans les autres Parties ». L'article 6 permet aux autorités compétentes de demander directement à un fournisseur de services situé sur le territoire d'une autre Partie des informations sur les noms de domaine enregistrés, et l'article 7 la divulgation de données relatives aux abonnés. La **section 3** («procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées») donne effet aux injonctions d'une autre Partie ordonnant la production accélérée de données (article 8) et la divulgation accélérée de données stockées en situation d'urgence (article 9). La **section 4** (article 10) fixe les «procédures relatives à la demande d'entraide urgente». Enfin, la **section 5** («procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables») autorise les vidéoconférences (article 11), et surtout les équipes communes d'enquête (ECE) et les enquêtes communes (article 12).

11. Le **chapitre III** traite des conditions et garanties (article 13), notamment pour ce qui est de la protection des données à caractère personnel (article 14). Ce sont surtout ce chapitre et la section 2 sur la coopération directe avec les fournisseurs de services qui ont suscité des critiques dans la société civile.

4. Critiques et recommandations émanant de parties prenantes

12. Le Conseil européen de la protection des données (EDPB)[4] critique dans sa contribution du 4 mai 2021[5] la brièveté du délai de soumission des observations sur le premier projet complet de Protocole, publié le 14 avril 2021. Il juge qu'il serait nécessaire de mieux analyser les projets de dispositions sur la protection des données, notamment leur compatibilité avec le Règlement général sur la protection des données (RGPD) et la jurisprudence de la Cour de justice de l'Union européenne (CJUE). Sur le fond, il recommande:

– de préciser dans le projet que les garanties relatives à la protection des données ont un caractère contraignant ;

– de garantir l'intervention systématique d'une autorité judiciaire ou d'une autorité administrative indépendante de la Partie requise, sauf en cas d'urgence valablement démontrée, et d'appliquer le principe de la double incrimination en conformité avec la jurisprudence de la CJUE ;

– de clarifier la définition des informations relatives aux abonnés de façon à en exclure les données relatives au trafic et au contenu ;

– de mieux définir les spécifications et exigences relatives à la sécurité et à l'authentification des organismes habilités à demander et à recevoir des données ;

– d'inclure l'application du principe de proportionnalité dans le texte de l'article 13 ;

– d'indiquer à l'article 14 que le projet de Protocole s'applique aux Parties, sauf autre accord ou arrangement entre les Parties concernées garantissant un niveau égal ou supérieur de protection de la vie privée et de la protection des données à caractère personnel à celui que prévoit le Protocole ;

– de préciser à l'article 14, paragraphe 1.a, que les données à caractère personnel figurant dans la demande et reçues par l'autorité ou l'entité privée requise bénéficient de la même protection que celles que reçoit l'autorité requérante ;

– de permettre à la Partie qui communique des données à caractère personnel (dans une demande ou en réponse à une demande) d'exiger de la Partie destinataire des garanties supplémentaires, ou de permettre à la Partie requise de refuser la communication dans le but de ne pas éroder la protection des données à caractère personnel prévue par le droit de l'Union européenne ;

---

4. Le Comité européen de la protection des données (EDPB) est un organe européen indépendant, qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre les autorités de l'Union européenne chargées de la protection des données. Il est institué par le règlement général sur la protection des données (RGPD), et son siège se situe à Bruxelles. Il se compose de représentants des autorités nationales chargées de la protection des données (autorités de contrôle nationales) et du Contrôleur européen de la protection des données (CEPD). (Qui sommes-nous? | Conseil européen de la protection des données (europa.eu).

5. EDPB contribution to the 6th round of consultations on the Draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime, Bruxelles, 4 mai 2021 (en anglais uniquement).

– de 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 ;

– remplacer, à l'article 14, paragraphe 4, les mots « considérées comme sensibles compte tenu des risques qu'elles comportent » par « qui permettent ou confirment l'identification unique d'une personne physique » ;

– de préciser à l'article 14, paragraphe 6, concernant les décisions automatisées, qu'outre l'intervention humaine, les garanties prévues par le droit interne des Parties autorisant ce type de traitement doivent garantir les droits et libertés de la personne concernée ; et d'ajouter au paragraphe 6 une disposition interdisant spécifiquement le traitement de données sensibles aux fins d'une prise de décision automatisée, à moins que le paragraphe 6 n'impose expressément des mesures protégeant suffisamment les droits et libertés et les intérêts légitimes de la personne concernée ;

– d'étendre expressément le champ d'application de l'article 14, paragraphe 8 (tenue de registres), à toutes les activités de traitement, en particulier le «stockage» ;

– d'ajouter à la liste des notifications aux personnes concernées prévues à l'article 14, paragraphe 11, les coordonnées du responsable du traitement ;

– de compléter les dispositions de l'article 14, paragraphe 12, de sorte que quiconque puisse demander et obtenir des informations sur le fait que des données à caractère personnel le ou la concernant sont ou non traitées ; d'actualiser le paragraphe 12.b, en indiquant qu'en règle générale, les informations relatives à l'accès et à la rectification sont fournies gratuitement aux personnes concernées ; et de clarifier et préciser les conditions dans lesquelles l'information et les droits des personnes concernées peuvent être restreints dans un souci de pleine conformité avec le droit de l'Union européenne, et en particulier de respect des critères de prévisibilité et de proportionnalité ;

– d'assurer le respect des garanties relatives aux données personnelles relevant par exemple des privilèges et immunités de certaines professions ;

– de clarifier l'article 14, paragraphe 13, sur les recours effectifs pour faire en sorte que la juridiction de chaque Partie à la Convention sur la cybercriminalité prévoie des voies de recours judiciaires et non judiciaires ouvertes à toute personne concernée.

13. L'Agence des droits fondamentaux de l'Union européenne (FRA) a signalisé son accord de principe au projet de Protocole:

> *«Elle juge qu'il répond au besoin d'un cadre juridique clair, prévisible et fonctionnel, qui favorise la coopération internationale dans les affaires de cybercriminalité et la collecte de preuves électroniques dans les enquêtes et procédures pénales relatives à des délits, et qu'il pose des limites juridiques, tout en accordant une attention particulière aux droits fondamentaux, notamment le droit à la protection des données à caractère personnel*[6]*».*

14. La FRA propose néanmoins des améliorations, en particulier:

– à l'article 11, paragraphes 1 et 5, mentionner le principe *ne bis in idem*, afin d'éviter la double peine d'un témoin en cas de parjure ou d'infraction similaire lorsque deux États lui ont fait prêter serment ou lui ont dispensé des avertissements ;

– à l'article 11, paragraphe 7, à propos de la vidéoconférence, prévoir les mesures de protection des témoins disponibles au niveau national (comme le brouillage du visage ou de la voix) ;

– à l'article 7, paragraphe 1, et à l'article 8, paragraphe 1, mieux assurer «l'égalité des armes» entre le ministère public et la défense en prévoyant qu'au niveau national, les autorités compétentes de la Partie contractante peuvent également agir au nom de la défense;

– à l'article 7, paragraphes 7 et 8, et à l'article 8, mieux préciser les motifs pour lesquels un prestataire de services peut légitimement refuser de divulguer des informations sur un abonné (la violation de droits fondamentaux dans l'État requérant ou requis devant être reconnue comme un motif valable).

---

6. Fundamental Rights Agency comments on the Second additional protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Draft Protocol version 2), mai 2021.

15. La publication du projet de Protocole a aussi suscité de vives critiques parmi des groupes de la société civile. En ce qui concerne la procédure adoptée par le comité de rédaction (T-CY), l'Electronic Frontier Foundation résume comme suit leurs objections:

> *«En 2018, près d'une centaine de groupes d'intérêt public ont appelé le Conseil de l'Europe à laisser la société civile apporter une contribution technique à la préparation du protocole. En 2019, le Conseil européen de la protection des données (EDPB) a lui aussi appelé le T-CY à veiller à une participation précoce et plus proactive des autorités chargées de la protection des données à la préparation du projet, un appel qu'il a jugé bon de réitérer cette année. Lorsqu'il a publiquement soumis le projet de texte du protocole, le T-CY n'a laissé que 2,5 semaines aux parties prenantes pour présenter leurs observations, délai trop court, de l'avis de l'EDPB, pour une analyse soigneuse. Cette version du protocole ne comprenait pas non plus les explications relatives aux garanties de protection des données, publiées ultérieurement, dans la dernière version du 28 mai, sans consultation publique. Même d'autres branches du Conseil de l'Europe, comme le comité consultatif de la Convention 108, ont ainsi eu du mal à apporter une contribution significative*[7]*».*

16. Sur le fond, un collectif de groupes de défense de la liberté de l'internet[8] a vigoureusement critiqué le projet de Protocole dans une lettre commune envoyée le 2 mai 2021 au Président de l'Assemblée, M. Rik Daems, et à d'autres organes du Conseil de l'Europe. Il estime que la section 2 menace l'État de droit en autorisant la «coopération directe» avec des entités privées, et en encourageant ainsi la divulgation volontaire de données personnelles telles que les informations relatives à l'enregistrement des noms de domaine et les informations sur les abonnés, sans obligation d'obtenir une décision de justice pour toute injonction de production émise en vertu du Protocole. Il critique par ailleurs le manque de transparence et l'absence de garanties contre le «changement de finalité» du traitement des données reçues en application du Protocole et contre le choix opportuniste de la juridiction *(forum shopping)* dans les enquêtes communes. Il recommande donc notamment:

– que toute injonction de production émise en vertu du Protocole, y compris son article 6 (demande d'informations concernant l'enregistrement d'un nom de domaine), doive obligatoirement être autorisée par la justice ;

– que les Parties au Protocole additionnel soient tenues d'adhérer au Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223, «Convention 108+») ;

– que le Protocole définisse l'incompatibilité évoquée à l'article 14, paragraphe 2.a, qui interdit aux États recevant des éléments de preuve de les traiter ultérieurement « dans un but incompatible », et d'inclure des garanties pour circonscrire ce «changement de finalité» ;

– que le Protocole inclue des garanties contre la sélection opportuniste de la juridiction *(forum shopping)* dans les enquêtes communes et par les équipes communes d'enquête pour empêcher les Parties de contourner les restrictions et interdictions de certaines mesures d'enquête prévues dans leur droit interne ;

– que les autorités de surveillance soient tenues de publier des données (au moins agrégées) sur l'emploi des mesures prévues par le Protocole et sur le nombre de personnes touchées par ces mesures.

17. Dans un document plus détaillé soumis à l'Assemblée le 29 juillet 2021[9], un groupe de défenseurs du droit à la vie privée sur internet manifeste une vigoureuse opposition aux principales dispositions du projet de Protocole, en particulier la coopération directe avec les fournisseurs de services visée aux articles 6 et 7:

> *«L'accès libre aux données relatives aux abonnés peut menacer les lanceurs d'alerte, les sources des journalistes, les dissidents, les personnalités politiques et d'autres personnes, tout en érodant des privilèges et immunités essentiels. Le projet de protocole cherche à édulcorer la nature sensible des données relatives aux abonnés, et crée une série de pouvoirs très étendus» (page 1).*

---

7. Voir Global Law Enforcement Convention Weakens Privacy & Human Rights | Electronic Frontier Foundation (eff.org), 8 juin 2021.
8. Electronic Frontier Foundation, European Digital Rights, IT-Pol Danemark, Al Sur, Article 19, Derechos Digitales et Homo Digitalis, Access Now, dataskyyd.net, Digital Rights Ireland, Digitale Gesellschaft, Fundacion Karisma, IPANDETEC Centroamerica, Vrijschrift.org.

18. Le document indique que, selon une enquête menée par le T-CY lui-même:

> *«de nombreux pays examinés exigent une autorisation de justice pour que les services de répression puissent accéder à certains types de données relatives aux abonnés. L'article 7 impose à ces États de poser des bases légales d'accès plus laxistes pour une autorité étrangère que pour leurs propres services de répression». (Page 4)*
>
> *«L'article 7 érode ainsi les normes de protection de la vie privée, même dans le cas où la protection est déjà suffisante. Nous recommandons donc que l'article 7 soit intégralement rayé du texte du protocole». (page 5)*

19. Il est également observé dans le document que:

> *«Imposer des limites de temps et de champ d'application au dispositif de réserves de l'article 7 oblige en fait les États à un niveau de protection particulier malgré l'évolution constante de la jurisprudence sur les informations relatives aux abonnés» (page 7). «Il est donc instamment demandé aux rédacteurs du Protocole de veiller à ce que les parties puissent exclure les informations relatives aux abonnés de l'article 7, au gré de l'évolution de la jurisprudence et de la législation, en admettant que des réserves et déclarations soient faites après la signature et la ratification du Protocole» (page 8).*

20. Les auteurs du document recommandent en outre l'introduction d'une obligation de notification ou de consultation des autorités de la Partie requise, de sorte qu'elles puissent le cas échéant appliquer les motifs de refus, et donner instruction au fournisseur de services de ne pas divulguer les informations relatives à l'abonné (recommandation 5, page 9). Ils voudraient aussi que les demandes de données relatives aux abonnés décrivent suffisamment les faits et justifient suffisamment la pertinence de la demande dans l'enquête pour qu'il soit possible d'apprécier convenablement ses effets sur les droits fondamentaux». (recommandation 6, page 10). Autre point important: le Protocole devrait prévoir que l'autorisation d'une juridiction indépendante constitue le seuil d'accès transfrontalier aux données relatives aux abonnés, ou au moins permettre aux Parties d'exiger une autorisation de cette nature (recommandation 7, page 11).

21. Le document critique vigoureusement aussi l'article 12 sur les enquêtes communes et les équipes communes d'enquête. Leur champ d'application et leur durée devraient être plus limités, elles devraient être soumises à autorisation des autorités centrales et ne pas pouvoir contourner les garanties fondamentales par sélection opportuniste de la juridiction *(forum shopping)* (pages 12-17). Il propose également un nouvel article 13b sur la confidentialité garantissant qu'il ne peut être fait un usage abusif des conditions de confidentialité des enquêtes (page 18).

22. Les auteurs sont en principe favorables à la présence de garanties détaillées dans le Protocole. Mais ils considèrent que:

> *«Le caractère facultatif de l'article 14 nuit à son utilité et contraste avec le caractère contraignant des obligations créées par le protocole en matière d'accès légal. L'un des aspects les plus problématiques du protocole et de sa Convention est qu'ils créent des obligations spécifiques en matière d'accès légal tout en ne formulant que de façon générale les garanties exigées en matière de droits humains et de respect de la vie privée, à préciser dans le droit national de chacun des signataires. […] Or ces dispositions ne garantissent pas un niveau de protection des données compatible avec les instruments modernes de protection des données, comme la Convention 108/108+». (pages 19-20)*

23. Enfin, le Conseil des barreaux européens (CCBE)[10] a émis des commentaires critiques et proposé des améliorations qu'il considère comme des «exigences minimales». Certaines sont similaires à celles de l'EDPB et de la FRA, notamment: créer un dispositif général de contrôle juridictionnel préalable assorti d'un cadre de protection du privilège attaché au secret de la communication entre l'avocat et son client et du secret professionnel; exiger la notification des autorités de l'État requis avant que les données ne soient communiquées à l'État requérant par le fournisseur de services auquel s'adresse l'injonction de produire ; clarifier et renforcer les motifs de refus d'exécution des injonctions internationales de production ; le fait que les données demandées sont couvertes par le secret de la communication entre avocat et client ou le secret professionnel doit constituer un motif absolu de refus ; faire en sorte que le suspect, le prévenu ou son avocat puissent demander une injonction internationale de production ou de conservation de manière aussi

---

9. Privacy & Human Rights in Cross-Border Law Enforcement, Joint Civil Society Comment to the Parliamentary Assembly of the Council of Europe (PACE) on the Second Additional Protocol to the Cybercrime Convention (CETS 185), by Derechos Digitales America Latina, Electronic Frontier Foundation, EDRI and cippic, 22 pages (disponible auprès du Secrétariat).

10. CCBE comments on the Draft Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (version 12 April 2021), 30 avril 2021.

péremptoire que les services répressif (principe de l'égalité des armes). Le CCBE est par ailleurs seul à demander que le Protocole prévoie expressément que l'avocat ait la possibilité de participer à l'audition en vidéoconférence pour défendre les intérêts de son client.

5. Évaluation des commentaires et propositions

24. Rappelons tout d'abord que le Protocole vise à améliorer les outils d'enquête et à rendre justice aux victimes. Eu égard à l'ampleur actuelle de la cybercriminalité et au faible nombre de sanctions infligées à ses auteurs, il importe d'améliorer les chances des victimes d'obtenir justice, et d'alourdir considérablement le risque de sanction pour les auteurs. La cybercriminalité (attaques par logiciel rançonneur, par exemple) a causé des préjudices économiques considérables, voire des pertes de vies humaines, certains criminels n'hésitant pas à s'attaquer aux hôpitaux et autres infrastructures essentielles. Comme l'ont montré de récents échanges entre les présidents des États-Unis d'Amérique et de la Fédération de Russie[11], la cybercriminalité menace même la paix mondiale. Les menaces implicites de représailles consécutives à des attaques contre des infrastructures essentielles, commises par des acteurs peut-être soutenus ou tacitement tolérés par des gouvernements, pourraient déclencher des tensions, avec des conséquences potentiellement dévastatrices.

25. Il convient également de rappeler que le Deuxième Protocole additionnel à la Convention Cybercriminalité est un instrument de justice pénale qui s'applique à des enquêtes ou procédures pénales spécifiques liées à la cybercriminalité et à la collecte de preuves sous forme électronique, comme l'indique l'article 2 relatif au champ d'application. Il n'est donc pas utilisable à des fins de sécurité nationale, ni de surveillance de masse ou de collecte de données à grande échelle. Il ne vise pas non plus à établir ni à harmoniser des régimes complets de protection des données. La Convention sur la cybercriminalité rassemble actuellement 66 Parties (dont 21 ne sont pas membres du Conseil de l'Europe et 40 ne sont pas membres de l'Union européenne). Le Protocole doit donc laisser une marge de manœuvre suffisante pour permettre une adaptation aux différents systèmes juridiques et à l'évolution de la technologie, des modèles économiques et de l'interprétation par les tribunaux[12].

26. Il pourrait ainsi se révéler impossible de reprendre intégralement l'acquis du Conseil de l'Europe et de l'Union européenne en matière de droit à la vie privée et de protection des données dans la Convention sur la cybercriminalité et ses Protocoles additionnels, et de lui donner un caractère contraignant pour toutes les Parties. Cela irait à contre-courant du but même de ces instruments — but qui touche à la protection de droits fondamentaux (ceux des victimes de la cybercriminalité) et, on l'a vu, au fonctionnement de l'État de droit et de la démocratie. Je suis donc largement d'accord avec le texte du Protocole tel qu'il nous est présenté par ses rédacteurs.

27. Cela étant, certaines propositions soumises par l'EDPB, la FRA et des groupes de la société civile comme l'Electronic Frontier Foundation (EFF) et le Conseil des barreaux européens (CCBE) n'en paraissent pas moins judicieuses: elles ne semblent pas compromettre le but du Protocole, mais améliorent concrètement la protection de toutes les personnes concernées. Voici une liste de ces améliorations possibles, établie à partir des 15 propositions que j'avais provisoirement jugées positives dans ma note introductive. À la lumière des apports des experts invités à notre audition en commission du 14 septembre, j'ai choisi de conserver les propositions suivantes:

1. faire figurer l'application du principe de proportionnalité dans le texte de l'article 13, outre sa mention dans le rapport explicatif[13]

Selon moi, le principe de proportionnalité joue un rôle central dans la protection des droits fondamentaux, et mérite une place dans le texte même du Protocole. Cela vaut même si le principe est évoqué dans le Rapport explicatif du projet de Protocole et que l'article 15 de la Convention sur la cybercriminalité, qui mentionne ce principe, est incorporé dans le projet de Protocole par le biais de son article 13. Sa mention dans le texte du Protocole lui-même constitue une proclamation résolue de ce principe fondamental des droits humains, qui aura donc un poids supplémentaire dans l'interprétation qui sera donnée au Protocole dans la pratique.

---

11. Voir par exemple https://nypost.com/2021/07/27/in-jab-at-putin-biden-warns-cyberattacks-could-cause-shooting-war. https://www.bbc.co.uk/news/world-us-canada-57786302, Putin Is Testing Biden's Cyber Resolve (foreignpolicy.com).
12. Voir Résumé des commentaires sur les avis des comités du Conseil de l'Europe et les soumissions d'autres parties prenantes sur le projet de deuxième protocole additionnel à la Convention sur la cybercriminalité (mai 2021), note préparée par le Secrétariat, T-CY (2021)12 du 28 mai 2021 («Document de synthèse»), pages 3-4.
13. Dans ce qui suit, les textes *en italique* résument les propositions des parties prenantes ; une brève évaluation préliminaire est ensuite donnée en caractères normaux.

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

Cette proposition reflète bien la formule usuelle de la Convention européenne des droits de l'homme telle qu'interprétée par la Cour dans l'évaluation des restrictions du droit à la vie privée garanti à l'article 8 de la Convention. Comme l'ont expliqué les experts du T-CY, on pourrait la juger techniquement «superflue», au même titre que la première proposition ci-dessus, mais elle adresse un message fort aux 47 États Parties à la Convention, ce qui devrait influencer l'interprétation future de cette disposition dans un sens favorable aux droits humains. Afin de tenir compte de la remarque des experts du T-CY, qui considèrent que les États qui ne sont pas Parties à la Convention peuvent employer des notions ou une terminologie différentes et pourraient être dissuadés de signer le projet de Protocole en raison de cette terminologie inspirée de la Convention, la proposition pourrait être complétée par les mots «ou assure par d'autres voies une protection adéquate des droits de l'homme et des libertés» (comme dans l'article 15 de la Convention incorporé par l'article 13 du projet de Protocole).

3. ajouter à la liste des notifications aux personnes concernées prévues à l'article 14, paragraphe 11, les coordonnées du responsable du traitement

Cela faciliterait l'exercice par la personne concernée de son droit à l'information et ne devrait pas représenter une charge importante pour les autorités compétentes.

4. actualiser le paragraphe 12.b de l'article 14 en indiquant qu'en règle générale, les informations relatives à l'accès et à la rectification sont fournies gratuitement aux personnes concernées

Le texte actuel du Protocole dit que « les frais d'accès doivent être limités à ce qui est raisonnable et non excessif ». Mais la bonne pratique observée dans de nombreux pays est que l'accès est gratuit, sauf abus manifeste (demandes répétées pour le même motif, par exemple).

5. assurer le respect des garanties relatives à des données personnelles relevant par exemple des privilèges et immunités de certaines professions

Les garanties liées aux privilèges et immunités de certaines professions (avocats, médecins, clergé, parlementaires, par exemple) devraient effectivement figurer expressément dans le projet de Protocole.

6. imposer aux autorités de surveillance de publier des données (au moins agrégées) sur l'emploi des mesures prévues par le Protocole et sur le nombre de personnes touchées par ces mesures

Cette proposition mérite notre soutien dès lors qu'elle se borne à des données agrégées. Elle favoriserait la transparence et ainsi la confiance du public dans les instruments créés par le Protocole et elle faciliterait l'évaluation du fonctionnement de cet instrument. La divulgation d'informations agrégées ne saurait nuire à des enquêtes en cours, ni se traduire par la divulgation de données personnelles sensibles.

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.

Ces propositions du CCBE sont pleines de bon sens, car les cybercriminels sont souvent des groupes organisés, connus pour menacer, voire éliminer les témoins, et le droit fondamental d'être assisté par un avocat doit également être respecté dans les auditions de preuves menées en vidéoconférence.

8. mieux assurer «l'égalité des armes» entre le ministère public et la défense en prévoyant qu'au niveau national, les autorités compétentes de la Partie contractante peuvent également agir au nom de la défense

Cette proposition est elle aussi sensée. Le respect des droits humains et de l'État de droit exige évidemment que l'accusé, présumé innocent, ait le même accès aux éléments de preuve que l'accusation.

28. D'autres propositions de parties prenantes, en revanche, semblent incompatibles avec la nature et le but du Protocole, à savoir créer, dans le domaine de la lutte contre la cybercriminalité, une plate-forme de coopération ouverte au plus grand nombre d'États possible, y compris ceux qui n'ont pas, ou pas encore, atteint le niveau de protection des données du RGPD de l'Union européenne ou de la Convention

européenne des droits de l'homme et de la Convention 108+ du Conseil de l'Europe. D'autres paraissent superflues, soit que le projet de Protocole les prenne déjà en compte, soit que les clarifications demandées figurent déjà dans le rapport explicatif du Protocole.

29. Cela vaut pour les propositions suivantes:

– *Supprimer l'article 7 sur les injonctions de divulgation adressées directement aux fournisseurs de services internet:* cela irait à l'encontre du but du Protocole en supprimant un moyen efficace de désengorgement des dispositifs actuels d'entraide judiciaire, qui passent par des autorités centrales nationales surchargées. La portée limitée des injonctions visées à l'article 7, les garanties prévues aux articles 13 et 14 et celles du droit pénal des Parties elles-mêmes devraient prévenir les atteintes au droit au respect de la vie privée.

– *Introduire une obligation de notification ou de consultation des autorités de la Partie requise pour la Partie requérante ou le fournisseur de services requis*: cette obligation représenterait une lourde charge administrative pour les Parties qui ne jugent pas nécessaire d'être systématiquement informées des demandes adressées aux fournisseurs de services ; cela irait à l'encontre du but du Protocole, qui doit désengorger les dispositifs existants.

– *Faire en sorte que les demandes de données relatives aux abonnés décrivent suffisamment les faits et justifient suffisamment la pertinence de la demande dans l'enquête pour qu'il soit possible d'évaluer convenablement ses effets sur les droits fondamentaux*: cela est inutile, car l'article 7.4. dit déjà que l'injonction doit indiquer le fondement juridique interne qui habilite l'autorité à donner une injonction, et préciser les dispositions juridiques et les sanctions applicables à l'infraction à l'origine de l'enquête ou des poursuites. Exiger des informations supplémentaires sur les faits ou la procédure et sur la pertinence des informations relatives à l'abonné dans l'enquête ou la procédure imposerait à l'autorité requérante et au fournisseur de services requis une charge excessive, eu égard à la portée limitée des demandes visée à l'article 7.

– *Préciser dans le projet que les garanties relatives à la protection des données ont un caractère contraignant:* toute règle contraignante autre que celles qui figurent déjà aux articles 13 et 14 du projet risque de faire obstacle à l'accès des États non membres de l'Union européenne ou du Conseil de l'Europe. Les garanties convenues par les rédacteurs du texte actuel sont une réelle avancée; elles demanderont des efforts considérables aux pays dont le régime de protection des données est plus faible.

– *Garantir l'intervention systématique d'une autorité judiciaire ou d'une autorité administrative indépendante de la Partie requise, sauf en cas d'urgence valablement démontrée*: cela pourrait aussi aller à contre-courant du but du Protocole. Les paragraphes 13 et 14 de l'article 14 du projet actuel prévoient « des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations », et que « chaque Partie dispose d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et effectives», et que lesdites fonctions «comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives». Y ajouter un contrôle préventif systématique pourrait aller à l'encontre du but recherché: une coopération internationale rapide et administrativement allégée dans la lutte contre la cybercriminalité. Je pense qu'il serait disproportionné d'exiger une autorisation de justice pour les demandes d'informations concernant l'enregistrement de noms de domaine, sachant que les demandes sont limitées à des enquêtes et procédures pénales spécifiques, et que la divulgation doit satisfaire aux conditions raisonnables prévues par le droit interne et respecter les garanties énoncées aux articles 13 et 14[14].

– *Mieux définir les spécifications et exigences relatives à la sécurité et à l'authentification des organismes habilités à demander et à recevoir des données*: il serait impossible d'imposer un système unifié allant au-delà de l'article 6, qui a pour but de fonder juridiquement le système d'accès aux informations relatives à l'enregistrement des noms de domaine développé au sein de l'Internet Corporation for Assigned Names and Numbers (ICANN). Les exigences des fournisseurs de services et celles de la justice pénale diffèrent énormément en matière de sécurité et d'authentification. Le projet de Protocole (articles 6 et 7) se borne donc à demander que les autorités compétentes exigent des niveaux appropriés de sécurité et d'authentification, mais laisse aux Parties le soin de détailler ces dispositions.

14. Voir Document de synthèse (note 9), section 4.1.3.

– *Clarifier la définition des informations relatives aux abonnés de façon à en exclure les données relatives au trafic et au contenu*: cela n'est pas nécessaire, car la notion d'informations relatives à l'abonné est bien définie dans la Convention Cybercriminalité (article 18.3.), que le projet de Protocole additionnel ne fait que compléter. D'ailleurs, les paragraphes 92 et 93 du rapport explicatif précisent déjà que les données relatives au trafic sont exclues de la définition des informations relatives aux abonnés.

– *Renforcer les règles de création et de fonctionnement des équipes communes d'enquête visées à l'article 12, notamment pour empêcher les équipes communes d'enquête et les enquêtes communes des Parties de contourner par sélection opportuniste de la juridiction (forum shopping) des dispositions de leur droit interne restreignant ou interdisant certaines mesures d'investigation, et exiger l'approbation des accords de création d'une ECE par les autorités centrales*: ce serait inutile, les Parties participantes ne pouvant faire que ce qui est autorisé par leur droit interne. Lorsqu'une mesure est à exécuter dans une Partie participant à une équipe commune d'enquête, les autorités de cette Partie déterminent si elles peuvent exécuter ladite mesure en fonction de leur droit interne ; l'ECE est soumise à tous les dispositifs de contrôle de la juridiction pénale concernée[15]. Les ECE se sont révélées être des outils efficaces de coopération internationale contre la criminalité organisée ; leur création et leur fonctionnement ne devraient pas être entravés.

– *Insérer un nouvel article 13b garantissant qu'il ne peut être fait un usage abusif de la confidentialité des enquêtes*: cela serait inutile, car l'article 14 paragraphe 12, du projet de Protocole prévoit un droit général d'accès et de rectification pour les personnes dont les données personnelles ont été reçues. Le point a. i. prévoit déjà que:

  «l'accès dans un cas particulier [peut] être soumis à l'application de restrictions proportionnées autorisées par [le] cadre juridique interne [de la Partie concernée], nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée».

– *Définir l'incompatibilité évoquée à l'article 14, paragraphe 2.a, qui interdit aux États recevant des éléments de preuve de les traiter ultérieurement «dans un but incompatible» et inclure des garanties pour circonscrire ce «changement de finalité»*: cela n'est pas nécessaire, car la notion de «but incompatible» est clairement explicitée aux paragraphes 227 et suivants du rapport explicatif. Sont compatibles les finalités évoquées à l'article 2, c'est-à-dire les «enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques», ainsi que la «collecte d'éléments de preuve d'une infraction pénale sous forme électronique».

– *Indiquer à l'article 14 que le projet de Protocole s'applique aux Parties, sauf autre accord ou arrangement entre les Parties concernées garantissant un niveau égal ou supérieur de protection de la vie privée et de la protection des données à caractère personnel que celui que prévoit le Protocole*: l'ajout risquerait là aussi de faire obstacle à la coopération entre des Parties dont le régime de protection des données n'a pas encore atteint le niveau du GDPR ou de l'article 8 de la Convention européenne des droits de l'homme.

– *Préciser à l'article 14, paragraphe 6, concernant les décisions automatisées, qu'outre l'intervention humaine, les garanties prévues par le droit interne des Parties autorisant un tel traitement doivent garantir les droits et libertés de la personne concernée*: cet ajout semble inutile, car les garanties générales visées aux articles 13 et 14 du projet de Protocole s'appliquent dès lors qu'il y a intervention humaine, ce que le texte actuel définit déjà comme l'une des «garanties appropriées» nécessaires.

– *Compléter les dispositions de l'article 14, paragraphe 12, de sorte que quiconque puisse demander et obtenir des informations sur le fait que des données à caractère personnel le ou la concernant sont ou non traitées*: il semble déjà en être ainsi puisque l'article 14, paragraphe 12.a.i., dit que la personne concernée a droit à une copie de la documentation conservée à son sujet, ainsi qu'à des informations sur le fondement juridique et les finalités du traitement, la conservation et les destinataires des données, ainsi que sur les possibilités de recours disponibles.

– *Clarifier l'article 14, paragraphe 13, sur les recours effectifs pour obtenir que la juridiction de chaque Partie à la Convention sur la cybercriminalité prévoie des voies de recours judiciaires et non judiciaires ouvertes à toute personne concernée*: là encore, cela semble déjà clair dans le texte actuel. Le

15. Voir Document de synthèse (note 9), section 4.1.10.

paragraphe 13 dit que «chaque partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article».

– *Faire en sorte que les Parties au Protocole additionnel soient tenues d'adhérer à la Convention 108+:* il est tout à fait souhaitable que le plus grand nombre possible de Parties à la Convention sur la cybercriminalité et à ses Protocoles additionnels soient également Parties à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et à ses Protocoles additionnels; mais en faire une obligation empêcherait la signature du Protocole par un certain nombre de Parties potentielles, dont la coopération à la lutte contre la cybercriminalité, but du Protocole, est tout aussi souhaitable. Je n'en suggère pas moins que l'Assemblée appelle dans son Avis tous les États désireux de signer ce Protocole à envisager de signer et de ratifier aussi la Convention 108+.

– *Souligner le principe «ne bis in idem», afin d'éviter la double peine d'un témoin en cas de parjure ou d'infraction similaire lorsque deux États lui ont fait prêter serment ou lui ont dispensé d'autres avertissements*: le principe «ne bis in idem» est en général reconnu en droit pénal national, et il est inutile de le réaffirmer dans le Protocole pour une situation très spécifique.

30. À la lumière de la présentation faite par les experts lors de notre audition du 14 septembre 2021[16], je m'abstiens également de retenir les propositions suivantes, auxquelles j'avais donné une première appréciation positive dans ma note introductive, à savoir:

1. préciser à l'article 14, paragraphe 1.a, que les données à caractère personnel figurant dans la demande et reçues par l'autorité ou l'entité privée requise bénéficient de la même protection que celles que reçoit l'autorité requérante

Je considérais au départ que cette clarification permettrait de combler une éventuelle «lacune», puisque les demandes elles-mêmes comportent souvent des données à caractère personnel qui doivent être protégées au même titre que les données reçues en réponse à cette demande. Mais comme les experts du T-CY l'ont souligné, l'article 14, paragraphe1, combiné au paragraphe 221 du rapport explicatif garantit déjà que l'article 14 s'applique à toutes les données à caractère personnel qu'une Partie reçoit en vertu du présent Protocole, y compris aux données qui font partie de la demande.

2. permettre à la Partie qui communique des données à caractère personnel (dans une demande ou en réponse à une demande) d'exiger de la Partie destinataire des garanties supplémentaires, ou permettre à la Partie requise de refuser la communication pour ne pas éroder la protection des données à caractère personnel prévue par le droit de l'Union européenne

Je pensais tout d'abord que cette clause de sauvegarde pourrait bien être nécessaire à la préservation de l'acquis de l'Union européenne en matière de protection des données, son absence risquant de créer un obstacle juridique à la participation des États membres de l'Union européenne au dispositif de coopération mis en place par le Protocole. Mais les experts du T-CY m'ont convaincu que le projet de Protocole répond aux exigences fondamentales de la législation européenne (en particulier de l'article 46 du RGPD et de l'article 37 de la directive en matière de protection des données dans le domaine répressif). Le fait de chercher à imposer aux États non membres de l'Union européenne une «photocopie» complète de la réglementation de l'UE en matière de protection des données pourrait bien rendre très problématique la ratification du texte par bon nombre d'entre eux. Toutefois, afin de répondre aux critiques légitimes, il serait utile que le rapport explicatif soit révisé à propos de l'article 14 pour mieux expliquer l'interrelation entre les différents régimes de protection des données prévus par cet article.

3. remplacer, à l'article 14, paragraphe 4, les mots « considérées comme sensibles compte tenu des risques qu'elles comportent » par « qui permettent ou confirment l'identification unique d'une personne physique »

Je considérais au départ que la nouvelle formulation proposée était moins subjective (« considérées comme sensibles» – par qui?) parce qu'elle mettait l'accent sur le risque principal, c'est-à-dire l'autorisation de l'identification ou la confirmation de l'identité d'une personne physique; mais les experts du T-CY m'ont convaincu du fait que la formulation existante, qui prend en compte tous les risques en présence, offre la

16. Voir annexe.

souplesse nécessaire pour s'adapter au domaine évolutif des données biométriques. En outre, selon eux, les propositions de modifications restreignent en réalité considérablement l'application des garanties. Cela va à l'encontre du but de protection que poursuit l'article 14 du projet de Protocole.

4. ajouter au paragraphe 6 une disposition interdisant spécifiquement le traitement de données sensibles aux fins d'une prise de décision automatisée, à moins que le paragraphe 6 n'impose des mesures garantissant convenablement les droits et libertés et les intérêts légitimes de la personne concernée

Je pensais tout d'abord que cette proposition tenait compte à juste titre des risques particuliers que présente la prise de décision automatisée qui utilise des données sensibles, ce qui exigeait l'existence de garanties adéquates. Mais les experts du T-CY ont mis en avant le fait que le paragraphe 6, dans son libellé actuel, prévoit déjà ces garanties et est conforme aux normes en vigueur, notamment à la Convention 108+.

5. supprimer les limites de temps et de champ d'application du dispositif de réserves de l'article 7

Je considérais au départ qu'il était effectivement souhaitable de laisser aux Parties une certaine marge de réaction, en cas d'évolution de la jurisprudence ou de la législation après la signature ou la ratification du Protocole. Mais je suis à présent convaincu que le fait d'autoriser des réserves et des déclarations après la signature et la ratification s'écarterait trop de la pratique établie par les États en matière de signature et de ratification des traités.

6. étendre explicitement le champ d'application de l'article 14, paragraphe 8 (tenue de registres) à toutes les activités de traitement, en particulier le «stockage»

Il est en effet important, par souci de transparence et de confiance des citoyens dans le mécanisme établi par le Protocole, que des registres soient tenus sur toutes les activités de traitement, ce qui doit englober le stockage des données, qui peut à son tour représenter une activité particulièrement risquée. Mais les experts du T-CY ont rappelé que l'article 25 de la directive européenne en matière de protection des données dans le domaine répressif et la Convention 108+ ne prévoient pas non plus cette exigence et m'ont convaincu que le fait d'imposer l'enregistrement détaillé de chaque activité de stockage constituerait une charge excessive qu'un certain nombre de Parties ne seraient pas prêtes à supporter.

7. clarifier et préciser les conditions dans lesquelles l'information et les droits des personnes concernées peuvent être restreints, cela dans un souci de pleine conformité avec le droit de l'Union européenne, et en particulier de respect des critères de prévisibilité et de proportionnalité

J'ai d'abord pensé que le projet de Protocole, dans sa forme actuelle, ne définissait pas assez clairement les motifs recevables de refus ou de limitation du droit d'accès et qu'il fallait par conséquent les préciser, comme le propose l'EDPB. Les experts du T-CY ont toutefois rappelé la liste des quatre critères limitatifs des restrictions imposées aux droits de la personne concernée à l'article 12: *premièrement*, les restrictions doivent être proportionnées et autorisées par le cadre juridique interne; *deuxièmement*, elles doivent encore être «nécessaires» au moment de la décision; *troisièmement*, elles doivent servir à protéger les droits et libertés d'autrui ou poursuivre d'autres objectifs importants d'intérêt public général; enfin, *quatrièmement*, elles doivent tenir dûment compte des intérêts légitimes de l'intéressé. Ce critère semble également être conforme à la législation européenne en matière de protection des données (par exemple, l'article 23, paragraphe 1, du RGPD) et à la Convention 108+.

8. mieux préciser les motifs pour lesquels un fournisseur de services peut légitimement refuser de divulguer des informations sur un abonné (parmi lesquels devraient figurer la violation de droits fondamentaux dans l'État requérant ou requis, ainsi que le fait que les données demandées sont couvertes par la confidentialité de la communication entre avocat et client)

J'étais au départ favorable à ces propositions de la FRA et du CCBE, car elles renforçaient nettement la crédibilité du projet de Protocole du point de vue des droits humains. Cette précision réduirait le risque que doit prendre un fournisseur de services en refusant de communiquer des données d'utilisateurs dans des cas douteux. Mais les experts du T-CY ont expliqué que le projet de Protocole, dans sa forme actuelle, laissait plusieurs choix aux Parties, notamment celui de conférer aux fournisseurs de services le pouvoir discrétionnaire illimité de refuser les injonctions, ou d'exiger la notification des autorités nationales des injonctions signifiées aux fournisseurs sur leur territoire et d'enjoindre au prestataire de ne pas se conformer à l'injonction sur la base des motifs de refus prévus à l'article 25, paragraphe 4, et à l'article 27, paragraphe 4, de la Convention Cybercriminalité, notamment le refus pour des raisons d'atteinte aux «intérêts essentiels»

(c'est-à-dire pour des considérations liées aux droits humains). Enfin, il ne serait pas possible d'établir une liste exhaustive de motifs, tandis qu'une clause générale mettrait les fournisseurs de services dans la situation difficile de devoir statuer eux-mêmes sur cette question.

6. Conclusions

31. Nous avons vu que le projet de Deuxième Protocole additionnel à la Convention sur la cybercriminalité n'est pas une entreprise purement technique. Il soulève des questions d'une grande importance touchant à l'État de droit et aux droits humains, en particulier dans celles de ses dispositions qui créent des possibilités de coopération directe avec des fournisseurs de services et des entités d'autres Parties. Mais le Protocole, ne l'oublions pas, sera encadré dans son fonctionnement par les systèmes de justice pénale des Parties, et assujetti à toutes leurs procédures, réglementations, méthodes de communication des données, conditions et garanties. Il en va de même pour la «coopération directe» prévue par les articles 6 et 7, qui exigent que chaque Partie crée au niveau national le fondement juridique nécessaire à l'exercice de ces pouvoirs.

32. Le but du projet de Protocole (faciliter la coopération internationale dans la lutte contre la cybercriminalité) vise directement à la préservation de l'État de droit et à la protection des droits fondamentaux des victimes de la cybercriminalité.

33. Les observations et propositions des parties prenantes sont à prendre au sérieux. Pour que le Protocole atteigne son but, les rédacteurs ne sauraient toutefois les retenir toutes. J'ai expliqué au chapitre 5 ci-dessus ma position sur un certain nombre de propositions essentielles. Si je suis favorable à certaines d'entre elles, je suis plus sceptique à l'égard de certaines autres. Le projet d'avis qui précède le présent exposé des motifs reflète mes conclusions au sujet de ces propositions, que j'ai finalisées à la lumière des présentations faites par les experts lors de la réunion de notre commission du 14 septembre 2021.

Annexe - Audition du 14 septembre 2021

Lors de la réunion de la commission du 14 septembre 2021, nous avons entendu les présentations des trois experts suivants:

– M^me^ Cristina Schulman (Roumanie), Présidente du Comité de la Convention sur la cybercriminalité (T-CY) en charge de la rédaction du Protocole,

– Alexander Seger, son secrétaire exécutif,

– M^me^ Katitza Rodriguez (Electronic Frontier Foundation/EFF).

M^me^ Schulman et M. Seger se prononcent tous deux en faveur du maintien inchangé de l'actuel projet de texte, tandis que M^me^ Rodriguez propose un certain nombre de modifications à apporter et rappelle les critiques formulées par la société civile à l'égard de certaines dispositions du projet de Protocole.

M^me^ Schulman présente le contexte dans lequel s'inscrit le projet de Protocole et considère qu'il doit être adopté rapidement. Elle explique le processus de négociation complexe et inclusif auquel ont participé des États de toutes les régions du monde dont les ordres juridiques diffèrent, notamment les 21 États qui ne sont pas membres du Conseil de l'Europe. Il importe que le Protocole fonctionne pour chacun d'entre eux. Elle fait remarquer que le projet de Protocole a été rédigé pour donner aux gouvernements les moyens de respecter leurs obligations positives de protéger les personnes contre les violations de leurs droits causées par la cybercriminalité. Elle ajoute que, d'après les rédacteurs du Protocole, cet objectif pourrait être atteint en prévoyant des outils supplémentaires qui permettront de mener des enquêtes en bonne et due forme et d'engager des poursuites grâce à une coopération renforcée entre les Parties à la Convention sur la cybercriminalité. Elle souligne que la cybercriminalité ne connaît aucune frontière et qu'elle a atteint un niveau de prolifération sans précédent jusqu'alors. Le Deuxième Protocole additionnel permettrait de relever un certain nombre de défis rencontrés à l'occasion des enquêtes menées sur ces infractions, comme les difficultés auxquelles se heurte l'obtention d'éléments de preuve électroniques, qui se trouvent dans de multiples États étrangers, voire dans des États inconnus, et sont détenus par des personnes morales privées. Le projet de Protocole, souligne-t-elle, vise donc principalement à permettre une coopération directe avec les fournisseurs de services et les autres entités, en vue de communiquer les informations relatives aux abonnés et les données qui ont trait à l'enregistrement des noms de domaine, à simplifier la procédure de production des informations relatives aux abonnés et des données de trafic provenant d'autres Parties et à améliorer la coopération internationale dans les situations d'urgence, notamment en créant des ECE et en établissant des dispositions applicables à la vidéoconférence lorsque les autres traités ne les règlent pas. M^me^ Schulman souligne que ces mesures devraient être soumises à un système de garanties particulièrement solide, notamment l'article 14 consacré à la protection des données à caractère personnel, une disposition conventionnelle sans équivalent en matière de justice pénale. Les conditions et les garanties de l'article 15 de la Convention sur la cybercriminalité, notamment le principe de proportionnalité, ont été incorporées dans le projet de Protocole par le biais de son article 13. Elle insiste en outre sur l'étroitesse du champ d'application du projet de Protocole: il traite d'enquêtes judiciaires particulières et de la réunion d'éléments de preuve électroniques au cours de la procédure engagée en matière de cybercriminalité. Le projet de Protocole n'est pas destiné à être un traité d'harmonisation des régimes juridiques relatifs à la protection des données, ni à régler les systèmes de cybersécurité ou à autoriser la surveillance à grande échelle. Le Protocole représente un texte soigneusement calibré, conçu pour être compatible avec les acquis du Conseil de l'Europe, mais également pour respecter les exigences de l'ensemble des autres Parties à la Convention Cybercriminalité. M^me^ Schulman souligne que le fait d'ouvrir à nouveau à la rédaction certains paragraphes de ce projet de texte pourrait nuire à ce compromis minutieux.

M. Seger rappelle que de nombreuses Parties prenantes, y compris celles que mentionnait la note introductive du rapporteur, ont été invitées lors des négociations et du processus de rédaction et ont été entendues à cette occasion. Les observations de la société civile et des autres parties prenantes ont été, soit reprises dans le projet de Protocole, soit jugées superflues ou irréalisables. Quant aux propositions mentionnées au paragraphe 21 de la note introductive du rapporteur, il souligne qu'elles ont toutes été prises en considération. Certaines d'entre elles ne présentaient aucune valeur ajoutée par rapport au minutieux projet de texte actuel. Ainsi, la proposition visant à mentionner tout particulièrement le principe de proportionnalité à l'article 13 n'est pas nécessaire, puisque toutes les conditions prévues à l'article 15 de la Convention contre la cybercriminalité – y compris le principe de proportionnalité, mais pas seulement – ont été incorporées dans le projet de Protocole. La deuxième proposition est elle aussi dépourvue d'intérêt, puisque le projet d'article 14, paragraphe 1 (a), pourrait être applicable à toutes «les données à caractère personnel [reçues] au titre du […] Protocole»; les demandes adressées à d'autres autorités publiques ne pourraient donc pas comporter la «lacune» alléguée au sujet des données à caractère personnel. La proposition suivante, qui concernait la définition et le caractère sensible des données biométriques au titre de

l'article 14, paragraphe 4, du projet de Protocole, a été rejetée par les rédacteurs, qui considéraient que le sens à donner au terme «sensible», une notion en constante évolution, variait d'un État Partie à l'autre. L'actuel projet de texte représente par conséquent un compromis qui permet une certaine souplesse d'interprétation et d'application dans la pratique. Faute de temps, M. Seger renvoie ensuite la commission et le rapporteur aux observations écrites consacrées au reste des propositions.

M[me] Rodriguez est en profond désaccord avec les deux intervenants précédents. Elle estime que le projet de Protocole n'impose pas de garanties essentielles claires et applicables à la collecte transfrontière des éléments de preuve et, surtout, regrette que les protections de la vie privée prévues dans le projet de Protocole soient pour la plupart facultatives, et non obligatoires. Les pouvoirs de police réglementés par le projet de Protocole sont excessivement intrusifs, notamment pour la «coopération directe» entre les autorités d'enquête d'un État Partie et les personnes morales privées qui détiennent des données privées sensibles (articles 7 et 12) dans un autre État. Elle propose de supprimer entièrement ces dispositions ou tout au moins de les améliorer, en prévoyant des garanties procédurales solides pour les demandes de données, comme le prévoit la Convention 108+. Cette convention doit rester l'instrument juridique qui fait autorité dans ce domaine, même pour ce projet de Protocole. Elle propose que l'adhésion au Protocole soit subordonnée à la signature de la Convention 108+. Elle se montre particulièrement préoccupée par la possibilité offerte par le projet de Protocole aux gouvernements de conclure des accords secrets bilatéraux ou multilatéraux et de mettre en place des dispositions qui seraient moins protectrices que les normes internationales établies, tout en utilisant les puissants outils fournis par le Protocole. Elle critique également les dispositions du Protocole relatives aux équipes communes d'enquête et pose une question à ce sujet à M. Seger. Ce dernier répond qu'une lecture attentive du texte de l'article 12 sur les équipes communes d'enquête montre que les rédacteurs du Protocole ont remédié en profondeur à toutes les préoccupations soulevées par M[me] Rodriguez au sujet de la durée d'un accord sur les équipes communes d'enquête et du droit applicable de la Partie dans laquelle des mesures d'enquête sont prises. En outre, il souligne que cet article, qui régit l'activité des équipes communes d'enquête, est soumis aux garanties des articles 13 et 14, comme l'ensemble des autres mesures prévues par le projet de Protocole.