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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 16173
13 mai 2025

Projet de troisième protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale

Rapport[1]
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Vladimir VARDANYAN, Arménie, Groupe du Parti populaire européen

Sommaire **Page**

A. Projet d'avis 2
B. Exposé des motifs par M. Vladimir Vardanyan, rapporteur 4
1. Introduction 4
2. Travaux antérieurs et actuels de l'Assemblée sur l'entraide judiciaire en matière pénale 4
3. Principales caractéristiques du projet de troisième protocole 5
4. Positions exprimées par différentes parties prenantes 8
5. La question de la surveillance étatique 8
5.1. Les arrêts de la Cour européenne des droits de l'homme 8
5.2. Les logiciels espions – constats et travaux des organes du Conseil de l'Europe 8
5.3. La surveillance étatique – teneur du projet de troisième protocole 10
6. Conclusions 11

1. Renvoi en commission: Doc. 16139, Renvoi 4865 du 7 avril 2025.

A. Projet d'avis[2]

1. L'Assemblée parlementaire se félicite de l'achèvement du projet de troisième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale (STE n° 30, «la Convention») par le Comité d'experts sur le fonctionnement des conventions européennes sur la coopération dans le domaine pénal et le Comité européen pour les problèmes criminels.

2. Depuis que la Convention a vu le jour en 1959, les activités criminelles sont devenues toujours plus transnationales. C'est pourquoi la coopération internationale, et en particulier la coopération transfrontalière, est essentielle pour lutter contre la criminalité transnationale, et celle-ci doit être aussi rapide, efficace et efficiente que possible. Dans le même temps, la coopération et l'entraide judiciaire en matière pénale doivent respecter les droits humains et l'État de droit, ce qui inclut, pour les États membres du Conseil de l'Europe, les normes de protection prévues par la Convention européenne des droits de l'homme (STE n° 5), en particulier le droit à un procès équitable et le droit au respect de la vie privée.

3. La Convention a été actualisée par des protocoles tous les vingt ans environ, le Premier Protocole additionnel (STE n° 99) ayant été ouvert à la signature en 1978 et le Deuxième Protocole additionnel (STE n° 182) en 2001, afin de répondre aux besoins pertinents de la coopération en matière pénale. Le projet de troisième protocole additionnel («le projet de troisième protocole») s'inscrit dans cette dynamique: il modernise opportunément la Convention, en reflétant l'utilisation des technologies modernes ainsi qu'en élargissant l'éventail des moyens par lesquels l'entraide judiciaire peut être demandée et en facilitant l'exécution des demandes d'entraide.

4. L'Assemblée se félicite de ce que le projet de troisième protocole tienne compte des évolutions technologiques modernes pour faciliter les demandes d'entraide judiciaire et les rendre plus économiques, notamment en donnant la priorité aux communications électroniques sécurisées dans les procédures de demande, en autorisant les auditions par vidéoconférence (avec les garanties appropriées) et en établissant des procédures visant à faciliter l'utilisation de dispositifs d'enregistrement lorsque la personne qui fait l'objet d'une enquête pénètre sur le territoire d'une autre Partie, ainsi qu'une procédure par laquelle les Parties peuvent présenter des demandes d'interception de télécommunications.

5. En ce qui concerne les auditions par vidéoconférence (article 2), l'Assemblée note que les Parties peuvent, à leur discrétion, appliquer cette possibilité aux auditions impliquant la personne poursuivie pénalement ou le suspect. Dans ce cas, les modalités de la vidéoconférence doivent faire l'objet d'un accord entre les Parties concernées, conformément au droit national et aux instruments internationaux pertinents (article 2, paragraphe 8). L'Assemblée note que cela doit se faire conformément au droit à un procès équitable consacré par l'article 6 de la Convention européenne des droits de l'homme et/ou d'autres dispositions similaires du droit international des droits humains. Cela implique que la personne poursuivie pénalement ou le suspect doit se voir garantir le droit de suivre la procédure sans obstacles techniques et le droit à l'assistance d'un défenseur, y compris la communication effective et confidentielle avec un avocat. Par souci de clarté, l'Assemblée propose que ces garanties soient explicitement mentionnées dans le projet de rapport explicatif du protocole relatif à l'article 2, paragraphe 8.

6. Une grande partie du projet de troisième protocole (articles 3 et 4) est destinée à faciliter la coopération internationale en matière de surveillance étatique. Le projet de texte améliore le cadre juridique de cette coopération en l'assortissant de garanties, telles que l'obligation pour l'État requérant d'indiquer la raison pour laquelle le but recherché par la mesure de surveillance ne peut être atteint de manière adéquate par d'autres moyens d'enquête, facilitant ainsi la vérification de sa proportionnalité, et la possibilité de refuser une demande au motif qu'une telle mesure n'aurait pas été autorisée par la législation de la Partie requise. L'Assemblée se félicite de ces garanties et note qu'elles visent également à couvrir le refus d'une demande pour des motifs tenant à l'État de droit ou aux droits humains, notamment sur la base de la Convention européenne des droits de l'homme.

7. Bien que favorable à la mise en place d'une base juridique pour la coopération internationale, assortie de garanties solides, l'Assemblée rappelle que la Cour européenne des droits de l'homme a relevé d'importantes lacunes dans la réglementation, le contrôle et le fonctionnement de la surveillance étatique dans plusieurs États membres, en violation du droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme. Un grand nombre de ces arrêts sont en attente d'exécution, ce qui montre que les problèmes constatés par la Cour européenne des droits de l'homme demeurent.

---

2. Projet d'avis adopté à l'unanimité par la commission le 13 mai 2025.

8. Dans le même ordre d'idées, dans sa Résolution 2513 (2023) «Le logiciel espion Pegasus et les autres types de logiciels similaires, et la surveillance secrète opérée par l'État», l'Assemblée a attiré l'attention sur le caractère très intrusif des logiciels espions modernes utilisés pour exercer une surveillance ciblée, et s'est déclarée profondément préoccupée par le fait que des logiciels espions avaient été utilisés illégalement ou à des fins illégitimes par plusieurs États membres. L'Assemblée a conclu que le recours à ce type de logiciels espions devrait être limité à des situations exceptionnelles, comme mesure de dernier ressort, et toujours sous contrôle juridictionnel.

9. De même, dans sa Recommandation 2258 (2023), l'Assemblée a demandé au Comité des Ministres d'adopter une recommandation aux États membres du Conseil de l'Europe sur la surveillance secrète et les droits humains, surtout à la lumière des menaces que présentent les nouvelles technologies de surveillance et les logiciels espions, et d'examiner la faisabilité d'une convention du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions. Le Comité des Ministres a convenu qu'un instrument non contraignant sur la surveillance secrète et les droits humains présenterait une réelle valeur ajoutée et a invité le Comité directeur pour les droits humains à en tenir compte dans ses travaux. En décembre 2024, la Commission européenne pour la démocratie par le droit («la Commission de Venise») a adopté, à la demande de l'Assemblée, un rapport intitulé «Rapport sur une réglementation des logiciels espions conforme à l'État de droit et aux droits humains». Elle y a conclu que les logiciels espions étaient des outils de surveillance intrusifs sans précédent qui ne devraient être développés et utilisés que dans des cadres juridiques pertinents répondant à des exigences strictes. Il ressort de cette étude que relativement peu d'États ont élaboré une législation qui réglemente spécifiquement l'usage des logiciels espions. Il n'est pas certain non plus que les États membres aient mis en place toutes les garanties minimales nécessaires.

10. Au vu de ces éléments, l'Assemblée recommande que le projet de troisième protocole soit adopté par le Comité des Ministres et ouvert à la signature et à la ratification. Dans le même temps, l'Assemblée demande instamment que des mesures soient prises d'urgence pour garantir que la surveillance étatique s'effectue selon des procédures qui respectent les normes internationales, faute de quoi la coopération internationale renforcée ne pourra qu'être entachée d'irrégularité. En particulier:

10.1. les États membres du Conseil de l'Europe devraient prendre les mesures nécessaires pour exécuter les arrêts de la Cour européenne des droits de l'homme concernant la surveillance étatique en adoptant les mesures générales requises;

10.2. les Etats membres du Conseil de l'Europe devraient veiller à ce que leur cadre juridique régissant le développement et l'utilisation de logiciels espions prévoie les garanties minimales définies par la Commission de Venise;

10.3. le Comité des Ministres devrait prendre des dispositions supplémentaires en vue de l'adoption d'une recommandation sur la surveillance secrète et les droits humains et d'un instrument contraignant sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions, à la lumière de la Recommandation 2258 (2023) de l'Assemblée;

10.4. les États non membres du Conseil de l'Europe qui sont Parties à la Convention et qui souhaitent devenir Parties au Troisième Protocole additionnel devraient aussi veiller à ce que leur cadre législatif en matière de surveillance étatique et son application soient conformes aux normes internationales des droits humains.

B. Exposé des motifs par M. Vladimir Vardanyan, rapporteur

1. Introduction

1. La Convention européenne d'entraide judiciaire en matière pénale (STE n° 30, «la Convention») a été ouverte à la signature en 1959 et est entrée en vigueur en 1962. Elle avait pour but de renforcer la coopération entre les États membres en matière d'enquêtes judiciaires, d'obtention de preuves et de poursuite des suspects. Au moment de son adoption, une grande partie de la Convention était consacrée aux moyens de coopération disponibles à l'époque, notamment à l'utilisation des commissions rogatoires pour demander la collecte et le transfert des preuves.

2. Depuis lors, deux protocoles additionnels sont venus actualiser la Convention. Le premier a été ouvert à la signature en 1978 (STE n° 99). Ce protocole a supprimé la possibilité qu'offrait la Convention de refuser l'entraide judiciaire au seul motif que la demande portait sur une infraction considérée comme relevant du domaine fiscal par la Partie requise. Il a aussi étendu la coopération internationale à la notification des actes visant à l'exécution d'une peine et à des mesures analogues. Enfin, il a complété la Convention par des dispositions relatives à l'échange de renseignements sur le casier judiciaire. Le Deuxième Protocole a été ouvert à la signature en 2001 (STE n° 182). Il avait pour but de renforcer la capacité des États à réagir à la criminalité transfrontalière en tenant compte des évolutions sociales, politiques et technologiques, notamment en élargissant l'éventail des situations dans lesquelles l'entraide judiciaire pouvait être demandée, en facilitant cette entraide et en la rendant plus rapide et plus souple.

3. Le Comité d'experts sur le fonctionnement des conventions européennes sur la coopération dans le domaine pénal (PC-OC), œuvrant sous l'autorité du Comité européen pour les problèmes criminels (CDPC), est chargé d'examiner le fonctionnement et la mise en œuvre des conventions et accords du Conseil de l'Europe dans le domaine de la coopération internationale en matière pénale, en vue de les adapter et d'en améliorer, le cas échéant, l'application pratique.

4. Dans l'exercice de ses responsabilités, le PC-OC a reconnu la nécessité d'actualiser plusieurs dispositions de la Convention et de son Deuxième Protocole additionnel, afin de tenir compte de l'évolution récente des pratiques et des systèmes utilisés dans le cadre de l'entraide judiciaire, comme le recours accru à la vidéoconférence et à d'autres outils technologiques. Il a également recensé les domaines dans lesquels les praticiens ont constaté des lacunes qu'il faudrait combler.

5. Après avoir examiné diverses approches, le PC-OC a décidé que l'adoption d'un protocole additionnel serait la solution la plus efficace et pratique pour moderniser la Convention en tenant compte de ces éléments. Cette proposition a obtenu l'approbation du CDPC, de sorte que l'élaboration d'un nouveau protocole à la Convention a été intégrée par le Comité des Ministres dans le mandat du PC-OC pour la période 2022-2025.

6. Sur la base des propositions formulées par plusieurs délégations, le PC-OC a élaboré un projet troisième protocole additionnel à la Convention («le projet de troisième protocole»). Le projet a été achevé lors de la 86e réunion (12-14 novembre 2024) du PC-OC, puis soumis au CDPC pour approbation. Le CDPC a passé en revue et approuvé le projet de troisième protocole lors de sa 86e session plénière (20-22 novembre 2024), et l'a transmis pour examen au Comité des Ministres.

7. Le 19 mars 2025, lors de leur 1523e réunion, les Délégués des Ministres ont décidé de soumettre le projet de troisième protocole à l'Assemblée parlementaire pour avis. La commission des questions juridiques et des droits de l'homme m'a désigné rapporteur lors de sa réunion du 7 avril 2025.

8. Dans le présent exposé des motifs, je résumerai les précédents travaux menés par l'Assemblée sur l'entraide judiciaire en matière pénale (section 2) et je présenterai les principaux aspects du projet de troisième protocole (section 3). J'aborderai brièvement l'absence de commentaire public sur le texte (section 4), avant d'examiner la question de la surveillance étatique (section 5). Enfin, je formulerai quelques conclusions (section 6).

2. Travaux antérieurs et actuels de l'Assemblée sur l'entraide judiciaire en matière pénale

9. L'Assemblée a précédemment formulé un avis sur la Convention originale (Avis 30 (1959)) ainsi qu'un avis sur le Deuxième Protocole additionnel à la Convention (Avis 231 (2001)).

10. L'Assemblée a adopté plusieurs résolutions et recommandations qui appelaient à des améliorations de l'entraide judiciaire afin qu'elle couvre un large éventail d'aspects de la criminalité. Parmi celles-ci figurent la Recommandation 1044 (1986) «Criminalité internationale», la Résolution 1147 (1998) «Criminalité des affaires: une menace pour l'Europe», la Recommandation 1507 (2001) «Lutte de l'Europe contre la criminalité économique et le crime organisé transnational: progrès ou recul?», la Recommandation 1531 (2001) «Sécurité et prévention de la criminalité dans les villes: création d'un observatoire européen», la Résolution 1785 (2011) et la Recommandation 1953 (2011) «L'obligation des États membres et observateurs du Conseil de l'Europe de coopérer pour réprimer les crimes de guerre», la Résolution 2038 (2015) et la Recommandation 2063 (2015) «La protection des témoins: outil indispensable pour la lutte contre le crime organisé et le terrorisme en Europe», qui insistent sur la nécessité de renforcer l'entraide judiciaire en matière de protection des témoins dans les affaires transfrontalières, la Résolution 2218 (2018) «Lutter contre le crime organisé en facilitant la confiscation des avoirs illicites» ainsi que la Résolution 2279 (2019) et la Recommandation 2154 (2019) «Lessiveuses: faire face aux nouveaux défis de la lutte internationale contre la criminalité organisée, la corruption et le blanchiment de capitaux». Elle a aussi adopté plusieurs textes appelant à coopérer et à engager des poursuites contre les auteurs des crimes internationaux commis dans le cadre de l'agression de la Fédération de Russie contre l'Ukraine, notamment la Résolution 2436 (2022) et la Recommandation 2231 (2022) «L'agression de la Fédération de Russie contre l'Ukraine: faire en sorte que les auteurs de graves violations du droit international humanitaire et d'autres crimes internationaux rendent des comptes» ainsi que la Résolution 2482 (2023), la Résolution 2556 (2024) et la Recommandation 2279 (2024) «Questions juridiques et violations des droits de l'homme liées à l'agression de la Fédération de Russie contre l'Ukraine».

3. Principales caractéristiques du projet de troisième protocole

11. Le projet de troisième protocole vise à renforcer la capacité des États membres et des États partenaires à lutter efficacement contre la criminalité. Il s'agit d'atteindre cet objectif en actualisant et en élargissant la portée de la Convention et de ses deux protocoles additionnels existants. La réalisation de cet objectif passe par la modernisation des dispositions qui régissent actuellement l'entraide judiciaire, l'élargissement du champ des moyens par lesquels l'entraide judiciaire peut être demandée, la facilitation de l'entraide et l'accroissement de sa rapidité et de sa souplesse. Grâce à ces améliorations, le projet de troisième protocole cherche à créer un cadre plus solide pour la coopération internationale en matière pénale, qui permettra aux États de relever plus efficacement les défis contemporains de la criminalité.

12. Les principales caractéristiques du projet de troisième protocole sont les suivantes:

– l'article 1 est consacré aux voies de communication devant être utilisées pour les demandes d'entraide judiciaire. Cet article modifie l'article 15 de la Convention, désignant les moyens de communication électronique sûrs comme la méthode à privilégier. L'article précise également quelles sont les autorités compétentes qui peuvent soumettre telle ou telle demande, selon son objet;

– l'article 2 concerne le recours à la vidéoconférence. Il tient compte de l'évolution des pratiques qui se sont développées pendant la pandémie de covid-19. Il dispose que les Parties à la Convention peuvent demander que l'audition ait lieu par vidéoconférence selon une procédure déterminée. La Partie requise accepte une telle audition à condition que l'utilisation de la vidéoconférence ne soit pas contraire aux principes fondamentaux de son droit et qu'elle dispose des moyens techniques permettant de procéder ainsi. Une liste de règles est exposée, établissant les garanties à respecter. Les Parties peuvent, si elles le souhaitent, recourir à la vidéoconférence dans les auditions auxquelles participe la personne poursuivie pénalement ou le suspect, mais seulement avec l'accord des autorités judiciaires compétentes et de la personne concernée, et conformément au droit national et aux instruments internationaux pertinents. Dans ce contexte, il convient de noter que la jurisprudence de la Cour européenne des droits de l'homme («la Cour») sur les auditions par vidéoconférence établit que la participation de l'accusé aux débats par vidéoconférence n'est pas, en soi, contraire à la Convention européenne des droits de l'homme (STE n° 5), mais que son application dans chaque cas d'espèce doit poursuivre un but légitime et que ses modalités de déroulement doivent être compatibles avec les exigences du respect des droits de la défense, tels qu'établis par l'article 6 de la Convention[3]. La Cour a également estimé que la personne poursuivie devait pouvoir suivre la procédure, être entendue sans obstacles techniques et avoir une communication effective et confidentielle avec un avocat[4]. Je pense que ces garanties pour la personne poursuivie pénalement ou le suspect devraient être explicitement mentionnées dans le projet de rapport explicatif relatif à l'article 2, paragraphe 8;

---

3. *Marcello Viola c. Italie*, Requête n° 45106/04, arrêt du 5 octobre 2006, paragraphe 67.
4. *Grigoryevskikh c. Russie,* Requête n° 22/03, arrêt du 9 avril 2009, paragraphe 83.

– l'article 3 définit les règles d'utilisation des dispositifs techniques d'enregistrement de position, de son ou de prise de vue sur le territoire d'une autre Partie. Cela concerne, par exemple, les situations dans lesquelles un traceur GPS a été installé sur le véhicule d'une personne faisant l'objet d'une enquête, un dispositif d'enregistrement audio a été mis en place ou un logiciel a été installé sur un appareil électronique portable. Lorsque le dispositif est déplacé dans une autre juridiction, il est souhaitable que les services répressifs puissent continuer à utiliser les données collectées par celui-ci. L'article dispose que, dans la mesure du possible, les demandes visant à poursuivre la surveillance sur le territoire d'une autre Partie devraient être faites à l'avance. Ces demandes doivent contenir un ensemble d'informations, concernant notamment l'autorité qui autorise la surveillance, son fondement juridique, sa nécessité, la personne visée par le dispositif, les modalités de mise en œuvre et la durée prévue. Les demandes peuvent être refusées au motif que l'enregistrement ne serait pas autorisé dans une affaire nationale similaire selon la législation de la Partie requise. Le rapport explicatif précise qu'un tel refus peut être fondé sur des préoccupations relatives aux droits humains, appréciées conformément à la législation de la Partie requise, notamment le droit au respect de la vie privée et familiale ou la protection contre toute discrimination fondée sur un motif prohibé. Les demandes peuvent aussi être refusées pour les motifs exposés aux articles 2 et 5 de la Convention. Ces motifs comprennent les cas dans lesquels la demande concerne une infraction que la Partie requise considère comme étant de nature politique ou comme étant liée à une infraction de nature politique, ou les cas dans lesquels la Partie requise considère que l'exécution de la demande pourrait porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de son pays;

– l'article 3 traite également des situations d'urgence dans lesquelles il n'est pas possible de présenter une demande avant qu'un dispositif technique d'enregistrement n'entre sur le territoire d'un autre pays. En pareil cas, la Partie qui utilise le dispositif doit immédiatement en notifier l'autre Partie en lui fournissant les mêmes informations que celles qui sont requises lorsque la demande est présentée à l'avance. Le dispositif peut rester actif dans l'attente de l'autorisation de la Partie notifiée. La Partie notifiée doit indiquer dès que possible, et au plus tard dans les quatre-vingt-seize heures, si le dispositif peut rester actif ou si elle valide son activité passée. Lorsque l'enregistrement ne serait pas autorisé dans un cas interne similaire selon la législation de la Partie requise, la Partie notifiée peut décider que l'enregistrement ne peut pas être effectué ou qu'il doit être interrompu. La procédure offre également à la Partie notifiée un large éventail de moyens de contrôle de l'activité: elle peut notamment exiger que tout matériel déjà enregistré pendant que la personne visée par le dispositif se trouvait sur son territoire ne soit pas utilisé, ou qu'il ne puisse l'être que sous certaines conditions; que la poursuite ou la validation de l'enregistrement soit subordonnée à la présentation d'une demande formelle d'entraide; ou que les données enregistrées sur son territoire soient partiellement ou totalement détruites. La Partie notifiante ne peut utiliser les enregistrements comme éléments de preuve dans une procédure pénale sans en avoir obtenu l'autorisation expresse de la Partie notifiée;

– l'article 3 donne aussi la possibilité aux Parties de déclarer qu'elles appliqueront certaines restrictions à la procédure de notification. Ces restrictions peuvent consister en une interdiction de collecter des données dans des domiciles privés et des lieux non accessibles au public, et/ou en une limitation de l'autorisation aux enquêtes relative à certaines infractions pénales;

– l'article 4 définit le cadre dans lequel les Parties peuvent demander à une autre Partie d'intercepter des télécommunications dans le contexte d'une enquête pénale. L'article exige que ces demandes contiennent des informations spécifiques, notamment une description précise de la télécommunication à intercepter, les données techniques pertinentes, la justification de la nécessité de la mesure, la confirmation de l'autorisation par l'autorité compétente de la Partie requérante et la durée prévue de l'interception. La Partie requise peut refuser d'exécuter la demande pour les mêmes motifs de refus que ceux qui sont prévus à l'article 3. La Partie requise peut également subordonner l'exécution des demandes à des conditions: elle peut exiger que les données enregistrées qui sont étrangères à l'affaire soient détruites, que la personne dont les télécommunications ont été interceptées en soit informée après la mesure, que l'utilisation des éléments de preuve soit limitée aux fins indiquées dans la demande, ou imposer toute autre condition applicable à une affaire nationale similaire. S'il y a lieu, la Partie requérante peut aussi demander la transcription, le décodage ou le décryptage des enregistrements, sous réserve de l'accord de la Partie requise. Les autorités judiciaires de la Partie requise peuvent détruire les parties des enregistrements jugées étrangères à l'affaire ou qui sont couvertes par la confidentialité des communications avant de les transmettre à la Partie requérante. Si la communication interceptée révèle qu'une infraction a été commise entièrement ou principalement sur le territoire de la Partie requise, la Partie requérante est encouragée à transmettre l'information afin de permettre les poursuites dans cette juridiction;

– l'article 5 du projet de troisième protocole fixe les règles relatives au paiement des frais engagés dans le cadre de l'entraide judiciaire. Il dresse la liste de frais spécifiques, qui seront remboursés par la Partie requérante à moins que les Parties n'en conviennent autrement. Outre ces frais, l'article dispose que les Parties ne se réclament pas mutuellement le remboursement des frais découlant de l'application de la Convention ou de ses protocoles, à l'exception des frais occasionnés par l'intervention d'experts sur le territoire de la Partie requise, des frais occasionnés par le transfèrement de personnes détenues et des frais importants ou extraordinaires. L'article 5 est identique à une disposition similaire du Deuxième Protocole à la Convention, à l'exception d'un changement: la liste des frais spécifiques qui seront remboursés par la Partie requérante a été étendue afin d'y inclure «les frais exposés par les exploitants d'installations de télécommunication ou les fournisseurs de services du fait de l'exécution des demandes d'interception de télécommunications, ainsi que les frais résultant de la transcription, du décodage et du déchiffrage des communications interceptées, le cas échéant»;

– l'article 6 traite de la question de l'exécution en temps utile des demandes d'entraide judiciaire en matière pénale. Il pose le principe général selon lequel ces demandes devraient être exécutées avec la même célérité et la même priorité que lorsqu'il s'agit d'une affaire nationale comparable. L'article reconnaît que certaines circonstances, telles que les délais de procédure, la gravité de l'infraction ou d'autres situations d'urgence peuvent nécessiter de fixer un délai d'exécution précis. Dans de tels cas, la Partie requise doit s'efforcer de respecter ce délai, dans la mesure du possible. Si la Partie requise n'est pas en mesure de respecter le délai fixé, elle doit en informer rapidement la Partie requérante par tout moyen disponible, après quoi les Parties peuvent se consulter sur les délais et les conditions appropriés;

– l'article 7 porte sur la protection des données, remplaçant l'article 26 du Deuxième Protocole additionnel. Il dispose que les données à caractère personnel transférées à la suite de l'exécution d'une demande formulée en vertu de la Convention ou de ses protocoles ne peuvent être utilisées par la Partie destinataire qu'aux fins de procédures auxquelles s'applique la Convention ou l'un de ses protocoles, pour des procédures judiciaires ou administratives directement liées aux procédures susmentionnées ou afin de prévenir un danger immédiat et sérieux pour la sécurité publique. Ces données peuvent être utilisées à d'autres fins si la Partie transférante ou la personne concernée y ont donné leur accord. Les Parties peuvent refuser de transférer des données à caractère personnel obtenues à la suite de l'exécution d'une demande formulée en vertu de la Convention ou de l'un de ses protocoles lorsque ces données sont protégées par leur législation nationale et/ou lorsque la Partie destinataire n'est pas liée par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n^{o} 108) telle que modernisée par le Protocole d'amendement à cette Convention (STCE n^{o} 223), à moins que la Partie destinataire ne s'engage à accorder aux données la protection requise par la Partie transférante. Toute Partie qui transmet des données à caractère personnel obtenues à la suite de l'exécution d'une demande formulée en vertu de la Convention ou de l'un de ses protocoles peut exiger de la Partie destinataire de l'informer de l'utilisation qui en a été faite. Enfin, toute Partie peut, par une déclaration, exiger que, dans le cadre de procédures pour lesquelles elle aurait pu refuser ou limiter la transmission ou l'utilisation de données à caractère personnel conformément aux dispositions de la Convention ou d'un de ses protocoles, les données à caractère personnel qu'elle transmet à une autre Partie ne soient utilisées par cette dernière qu'avec son accord préalable;

– les autres articles du projet de troisième protocole concernent: le règlement amiable des difficultés relatives à l'interprétation de la Convention et de ses protocoles (article 8); les relations entre les dispositions du projet de troisième protocole et les dispositions existantes de la Convention et de ses protocoles additionnels (article 9); les principes régissant la signature du Protocole par les Parties et son entrée en vigueur (article 10); l'adhésion au Protocole (article 11); son application territoriale (article 12); les réserves et déclarations (article 13); la dénonciation (article 14); et les notifications (article 15). Les articles 10 à 15 se fondent sur le «Modèle de clauses finales pour les conventions, protocoles additionnels et protocoles d'amendement conclus au sein du Conseil de l'Europe», qui a été adopté par le Comité des Ministres le 5 juillet 2017, ainsi que sur les clauses finales de la Convention;

– l'article 13 dispose qu'il n'est possible de formuler des réserves qu'à l'égard des articles 3 et 4 du projet de troisième protocole. Les Parties peuvent se prévaloir du droit de ne pas accepter, en tout ou en partie, l'un ou l'autre de ces articles, ou les deux.

4. Positions exprimées par différentes parties prenantes

13. Aucune association de juristes ou autre organisation non gouvernementale n'a été représentée lors des réunions du PC-OC au cours desquelles le projet de troisième protocole a été élaboré. Il convient de noter qu'aucune organisation de la société civile n'a participé au processus de rédaction du projet de troisième protocole – et que le texte n'a fait l'objet d'aucun commentaire public. Dans ce contexte, il y a un manque d'informations et d'analyses sur les questions importantes reflétées dans le projet de protocole, y compris les questions relatives à l'utilisation de la surveillance opérée par l'État.

5. La question de la surveillance étatique

14. Le projet de troisième protocole a une incidence sur une question touchant aux droits fondamentaux qui a particulièrement retenu l'attention de l'Assemblée ces dernières années: l'utilisation de logiciels espions et d'autres moyens de surveillance étatique.

5.1. Les arrêts de la Cour européenne des droits de l'homme

15. La Cour européenne des droits de l'homme a rendu de nombreux arrêts sur la question générale de la surveillance étatique et a mis en évidence les pratiques qui étaient contraires à l'article 8 de la Convention européenne des droits de l'homme. Il est cependant très préoccupant de constater que bon nombre des arrêts en question sont toujours en attente d'exécution, ce qui signifie que le Comité des Ministres du Conseil de l'Europe n'a pas encore reçu suffisamment d'éléments démontrant que le problème qui a causé la violation des droits humains a été résolu. Parmi les arrêts en attente d'exécution figurent ceux dans lesquels la Cour a constaté que les garanties contre l'utilisation abusive de la surveillance secrète étaient insuffisantes (*Ekimdzhiev et autres c. Bulgarie*[5], *Zoltan Varga c. Slovaquie*[6], *Bucur et Toma c. Roumanie*[7], *Iordachi et autres c. République de Moldova*[8],et *Pietrzak et Bychawska-Siniarska et autres c. Pologne*[9]), que le raisonnement ayant conduit les juridictions internes à autoriser des mesures de surveillance était inapproprié (*Simic c. Serbie*[10],*Potoczka et Adamco c. Slovaquie*[11]), que les tiers dans une procédure pénale n'avaient pas eu la possibilité de contester la mise sur écoute téléphonique (*Contrada c. Italie (n° 4)*[12],*Pruteanu c. Roumanie*[13]), et que les données téléphoniques d'un avocat avaient été interceptées de manière injustifiée (*Bersheda et Rybolovlev c. Monaco*[14]).

5.2. Les logiciels espions – constats et travaux des organes du Conseil de l'Europe

16. Si la Cour européenne des droits de l'homme n'a pas encore statué sur l'utilisation des logiciels espions, le recours à ces derniers représente, en revanche, un sujet de préoccupation majeure pour l'Assemblée et la Commission européenne pour la démocratie par le droit (Commission de Venise).

17. Dans sa Résolution 2513 (2023) «Le logiciel espion Pegasus et les autres types de logiciels similaires, et la surveillance secrète opérée par l'État», l'Assemblée a noté que selon plusieurs rapports d'enquête, les gouvernements de plusieurs États membres du Conseil de l'Europe avaient acquis et utilisé Pegasus pour exercer une surveillance ciblée, et que d'autres États membres avaient acquis ou utilisé des logiciels espions similaires, tels que Candiru et Predator. Les logiciels espions peuvent être extrêmement intrusifs, donnant à l'utilisateur un accès complet et illimité à tous les capteurs et à toutes les informations de l'appareil ciblé. Ils transforment le smartphone en dispositif de surveillance 24 heures sur 24, en accédant à l'appareil photo et au microphone, aux données de géolocalisation, aux courriers électroniques, aux messages, aux photos, aux vidéos, aux mots de passe et aux applications. L'Assemblée s'est dite profondément préoccupée par le fait que des logiciels espions avaient été utilisés illégalement ou à des fins illégitimes par plusieurs États membres, notamment contre des journalistes, des opposants politiques et des défenseurs des droits humains. Elle a estimé que la surveillance secrète des opposants politiques, des agents publics, des

5. Requête n° 70078/12, arrêt du 11 janvier 2022.
6. Requête n° 58361/12, arrêt du 20 juillet 2021.
7. Requête n° 40238/02, arrêt du 8 janvier 2013.
8. Requête n° 25198/02, arrêt du 10 février 2009.
9. Requêtes n°s 72038/17 et 25237/18, arrêt du 28 mai 2024.
10. Requête n° 9172/21, arrêt du 14 janvier 2025.
11. Requête n° 7286/16, arrêt du 12 janvier 2023.
12. Requête n° 2507/19, arrêt du 23 mai 2024.
13. Requête n° 30181/05, arrêt du 3 février 2015.
14. Requête n° 36559/19, arrêt du 6 juin 2024.

journalistes, des défenseurs des droits humains et des acteurs de la société civile à des fins autres que celles énumérées de manière exhaustive à l'article 8.2 de la Convention européenne des droits de l'homme constituait une violation manifeste du droit au respect de la vie privée (article 8).

18. L'Assemblée a conclu que l'utilisation de logiciels espions devrait être limitée à des situations exceptionnelles et, comme mesure de dernier ressort, pour prévenir ou enquêter sur un acte précis constituant une menace réelle et sérieuse pour la sécurité nationale ou un crime grave spécifique et précisément défini, en ciblant uniquement la personne soupçonnée d'avoir commis ou prévu de commettre ces actes, et qu'elle devrait toujours être soumise à un contrôle juridictionnel. Afin de limiter un niveau d'intrusion aussi élevé, les États devraient tenir compte de la proportionnalité des nouveaux logiciels espions avant de les acquérir et de les utiliser; ils devraient également envisager d'utiliser des logiciels espions dépourvus de certaines des caractéristiques les plus invasives de Pegasus ou une version programmée de telle sorte qu'elle limite l'accès au strict nécessaire.

19. L'Assemblée a appelé les États membres qui semblaient avoir acquis ou utilisé Pegasus, notamment l'Allemagne, la Belgique, le Luxembourg et les Pays-Bas, à clarifier le cadre de son utilisation et les mécanismes de contrôle applicables. Elle les a invités à envoyer ces informations, ainsi que toute statistique sur l'utilisation de Pegasus, à l'Assemblée et à la Commission de Venise dans un délai de trois mois. L'Assemblée a également demandé à la Commission de Venise d'évaluer le cadre législatif et la pratique en matière de surveillance ciblée de tous les États membres afin de déterminer si ce cadre contenait des garanties appropriées et effectives contre tout abus éventuel de logiciels espions.

20. Dans sa Recommandation 2258 (2023), l'Assemblée a demandé au Comité des Ministres d'adopter une recommandation aux États membres du Conseil de l'Europe sur la surveillance secrète et les droits humains, surtout à la lumière des menaces que présentent les nouvelles technologies de surveillance et les logiciels espions, d'examiner la faisabilité d'une convention du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions et de coordonner ses initiatives avec d'autres organisations internationales à des fins d'établissement de normes et de coopération. Dans sa réponse à la recommandation de l'Assemblée, datée du 4 septembre 2024 (Doc. 16030), le Comité des Ministres a considéré qu'une recommandation sur la surveillance secrète et les droits humains était envisageable et présenterait une réelle valeur ajoutée, et a invité le Comité directeur pour les droits humains (CDDH) à tenir compte de cela pour l'examen à mi-parcours de son mandat. En novembre 2024, le CDDH a demandé au Comité des Ministres de lui donner pour mandat d'élaborer un instrument non contraignant sur les droits humains, l'usage des logiciels espions et la surveillance secrète par l'État[15].

21. En décembre 2024, la Commission de Venise a adopté, à la demande de l'Assemblée, un rapport intitulé «Rapport sur une réglementation des logiciels espions conforme à l'État de droit et aux droits humains». Elle y a conclu que les logiciels espions étaient «des outils de surveillance intrusifs» et qu'il était «essentiel de définir clairement les contours de l'utilisation des logiciels espions par les États afin de prévenir et d'éradiquer les pratiques abusives». La Commission de Venise a estimé que le développement et l'utilisation de logiciels espions ne devaient être possibles que si le cadre juridique en la matière répondait à certaines exigences et a dressé une liste exposant 11 garanties minimales à respecter, parmi lesquelles figurent les suivantes: l'utilisation de logiciels espions doit être régie par la législation primaire, qui doit clairement définir le champ d'application (restreint) *ratione materiae*, *personae* et *temporis* de la surveillance ciblée au moyen d'un logiciel espion. Les autorités requérantes (services répressifs ou services de renseignement) doivent toujours démontrer que les informations recherchées dans le cadre de l'enquête sont nécessaires à la réalisation du but légitime et qu'elles ne peuvent être obtenues par des moyens moins intrusifs. Il doit exister des procédures d'autorisation *ex ante* bien réglementées devant un tribunal ou un autre organe indépendant et la durée des mesures de surveillance doit être limitée au strict nécessaire. L'ensemble du processus de surveillance doit être soutenu par des institutions de contrôle externes indépendantes et efficaces, dotées de ressources suffisantes, qualifiées et spécialisées, et ne peut être confié exclusivement à l'exécutif. Les personnes surveillées doivent être informées ultérieurement, sauf exceptions définies par la loi, de sorte qu'elles puissent être parties prenantes dans le contrôle et la contestation de la mesure[16].

22. Bien que la Commission de Venise n'ait pas évalué au cas par cas si le cadre législatif de chaque État membre respectait l'ensemble des garanties minimales ainsi énoncées, le rapport laisse à penser que nombre d'entre eux ne les ont pas encore toutes mises en place. En fait, relativement peu d'États ont élaboré une législation qui réglemente spécifiquement l'usage des logiciels espions. L'Assemblée restera saisie de cette

15. CDDH(2024)R101.
16. Commission de Venise, Rapport sur une réglementation des logiciels espions conforme à l'État de droit et aux droits humains, 13 décembre 2024.

question importante, notamment par le biais des travaux de suivi de Pieter Omtzigt (Pays-Bas, PPE/DC), rapporteur chargé du suivi de la Résolution 2513 (2023) «Le logiciel espion Pegasus et autres types de logiciels similaires et la surveillance secrète opérée par l'État» pour la commission des questions juridiques et des droits de l'homme.

5.3. La surveillance étatique – teneur du projet de troisième protocole

23. De nombreuses dispositions du projet de troisième protocole ont pour effet d'établir de nouvelles procédures de coopération entre les Parties pour exercer une surveillance électronique. L'article 3 instaure une procédure visant à faciliter la poursuite de la surveillance lorsqu'une Partie a mis en place une surveillance électronique à l'égard d'une personne et que celle-ci se déplace sur le territoire d'une autre Partie. L'article 4 instaure une procédure permettant à une Partie de demander à une autre Partie d'intercepter les télécommunications d'une personne. L'article 5 dispose que les frais d'interception des télécommunications seront remboursés par la Partie qui a demandé l'interception.

24. Les logiciels espions ne sont explicitement mentionnés dans aucune de ces dispositions, mais selon le projet de rapport explicatif, l'article 3 vise à couvrir la possibilité de continuer à utiliser des logiciels installés sur des appareils électroniques portables sur le territoire d'une autre Partie. Les logiciels espions entrent clairement dans le champ d'application de cette disposition.

25. Il est très important que les services répressifs puissent exercer une surveillance dans les situations transfrontalières – à condition qu'ils le fassent uniquement dans des cas précis et avec les garanties appropriées.

26. Il existe des raisons de conclure que le projet de troisième protocole renforce les garanties procédurales régissant la surveillance électronique. En effet, si les demandes d'entraide judiciaire visant à autoriser la surveillance électronique transfrontalière sont déjà possibles dans le cadre de la Convention existante et de ses protocoles, les dispositions du projet de troisième protocole établissent des procédures qui sont spécifiquement adaptées à l'utilisation de la surveillance électronique et qui prévoient des garanties supplémentaires. En particulier, l'article 3 (sur l'utilisation de dispositifs techniques d'enregistrement sur le territoire d'une autre Partie) et l'article 4 (sur les demandes d'interception de télécommunications) prévoient des garanties qui présentent des caractéristiques particulières. Premièrement, les Parties au Protocole peuvent choisir de n'accepter aucun de ces articles, en tout ou en partie. Deuxièmement, en ce qui concerne l'article 3, les Parties peuvent déclarer que la procédure de notification ne peut être utilisée pour la collecte de données dans des domiciles et des lieux privés et/ou que la procédure de notification ne peut être utilisée que pour une liste limitée d'infractions[17]. Troisièmement, en vertu de l'article 3 et de l'article 4, les États requérants doivent justifier que les mesures ont été ordonnées légalement et que le but recherché par l'utilisation du dispositif technique d'enregistrement ou l'interception des télécommunications ne peut être atteint de manière adéquate par des mesures moins intrusives, c'est-à-dire que la surveillance est utilisée comme mesure de dernier recours. Quatrièmement, l'article 3 et l'article 4 instaurent une garantie qui n'existe pas dans la plupart des cas pour d'autres objets de demandes d'entraide judiciaire, à savoir que les Parties peuvent choisir de refuser une demande lorsque la même demande n'aurait pas été acceptée dans une affaire nationale similaire selon la législation de la Partie notifiée.

27. On peut ainsi observer que le projet de troisième protocole prévoit un plus large éventail de motifs permettant à une Partie de refuser d'autoriser la surveillance électronique sur son territoire: soit parce qu'elle a déclaré qu'elle n'accepterait pas les demandes d'entraide judiciaire dans de tels cas; soit en décidant qu'une telle demande doit être refusée, par l'application de son propre droit interne aux circonstances de l'espèce (y compris au motif qu'elle ne respecte pas les normes en matière de droits humains), ce qui n'est pas possible pour d'autres objets de demande d'entraide judiciaire.

28. Il importe également de noter que le projet de troisième protocole n'aura aucune incidence sur les actions des États menant des opérations clandestines ou de renseignement. Les États ne pourront y recourir que lorsqu'ils seront engagés dans une procédure pénale. Par conséquent, en établissant une procédure supplémentaire pour la surveillance technologique, qui comporte des garanties supplémentaires qui n'existaient pas auparavant, le projet de troisième protocole peut exposer cette surveillance à un examen supplémentaire.

---

17. Les infractions dont il est question sont celles qui sont énumérées à l'article 17, paragraphe 7 du Deuxième Protocole additionnel à la Convention, à savoir: l'assassinat, le meurtre, le viol, l'incendie volontaire, la fausse monnaie, le vol et recel aggravés, l'extorsion, l'enlèvement et la prise d'otage, le trafic d'êtres humains, le trafic illicite de stupéfiants et substances psychotropes, les infractions aux dispositions légales en matière d'armes et explosifs, la destruction par explosifs, le transport illicite de déchets toxiques et nuisibles, le trafic d'étrangers et l'abus sexuel d'enfant.

29. Dans le même temps, l'adoption même du projet de troisième protocole soulève aussi des inquiétudes – non pas en raison des dispositions du texte même, mais du contexte général de la réglementation de la surveillance étatique en Europe. Comme indiqué plus haut, il existe des lacunes importantes et largement répandues dans la réglementation de la surveillance étatique en général (comme l'indiquent les arrêts de la Cour européenne des droits de l'homme qui n'ont pas encore été exécutés), et de l'utilisation des logiciels espions en particulier (comme en témoignent les rapports de l'Assemblée et les avis de la Commission de Venise). Le projet de troisième protocole établit formellement une procédure juridique pour l'utilisation de la surveillance étatique dans des contextes transfrontaliers. Les États membres du Conseil de l'Europe institutionnalisent donc la coopération en matière de surveillance étatique à un moment où la plupart des États n'ont manifestement pas de réglementation adéquate en la matière. Cette initiative vient à point nommé pour rappeler aux États qu'il est nécessaire de redoubler d'efforts pour que l'utilisation de la surveillance étatique soit assortie de garanties adéquates – non seulement dans leur propre pays, mais aussi dans les pays avec lesquels ils coopèrent en matière pénale.

6. Conclusions

30. Les déplacements constants de personnes à travers les frontières, ainsi que le caractère transnational des activités et des organisations criminelles, font que les États ne peuvent pas lutter efficacement contre la criminalité sans coopérer les uns avec les autres. Il est essentiel que cette coopération soit aussi efficiente et efficace que possible, tout en maintenant les garanties nécessaires pour protéger les droits fondamentaux. La Convention a été créée en 1959 et a été actualisée par des protocoles additionnels tous les vingt ans environ: la première fois en 1978, la deuxième fois en 2001, et la troisième fois aujourd'hui en 2025. L'Assemblée devrait se féliciter de ce travail de modernisation de la Convention pour tenir compte de l'utilisation des technologies modernes.

31. Le projet de troisième protocole remplit cette mission en désignant les communications électroniques sécurisées comme le moyen privilégié de transmission des demandes d'entraide judiciaire en matière pénale, en officialisant et en facilitant l'utilisation de la vidéoconférence pour les auditions, en définissant des règles pour l'utilisation de dispositifs d'enregistrement électronique sur le territoire d'autres États et en officialisant un système par lequel une Partie peut demander à une autre Partie d'intercepter des communications électroniques sur son territoire. Ce sont toutes là des mesures importantes qui arrivent à point nommé pour permettre une coopération rapide et efficace en matière pénale.

32. Le projet de troisième protocole améliore le cadre juridique de la coopération internationale en vue de faciliter la surveillance étatique tout en l'assortissant de garanties appropriées. Dans le même temps, dans un contexte où la réglementation de la surveillance étatique est insuffisante dans de nombreux États européens – notamment en ce qui concerne les logiciels espions – l'adoption du projet de troisième protocole devrait servir de signal d'alarme pour rappeler aux États qu'ils doivent redoubler d'efforts pour mieux réglementer la surveillance étatique.

33. Compte tenu de ces éléments, je suggère à l'Assemblée d'accueillir favorablement le projet de troisième protocole, tout en soulignant qu'il doit s'accompagner d'efforts renouvelés pour veiller à ce que la surveillance étatique soit exercée de manière appropriée. Cela suppose notamment d'exécuter intégralement et dans les délais impartis les arrêts de la Cour européenne des droits de l'homme, d'adopter des cadres juridiques pour le développement et l'utilisation de logiciels espions incluant les garanties minimales définies par la Commission de Venise, d'adopter une recommandation sur la surveillance secrète et les droits humains, et d'élaborer un instrument juridiquement contraignant du Conseil de l'Europe sur l'acquisition, l'utilisation, la vente et l'exportation de logiciels espions.