



Doc. 16173

13 May 2025

Draft third additional protocol to the European Convention on Mutual Assistance in Criminal Matters

Report¹

Committee on Legal Affairs and Human Rights

Rapporteur: Mr Vladimir VARDANYAN, Armenia, Group of the European People's Party

Contents	Page
A. Draft Opinion	2
B. Explanatory memorandum by Mr Vladimir Vardanyan, rapporteur	4
1. Introduction	4
2. Previous and current work of the Assembly on mutual assistance in criminal matters	4
3. Main features of the draft third protocol	5
4. Positions voiced by different stakeholders	7
5. The issue of State surveillance	7
5.1. Judgments of the European Court of Human Rights	7
5.2. Spyware – findings and work of Council of Europe bodies	8
5.3. State surveillance – contents of the draft third protocol	9
6. Conclusions	10

1. Reference to committee: [Doc. 16139](#), Reference 4865 of 7 April 2025.



A. Draft Opinion²

1. The Parliamentary Assembly welcomes the finalisation of the draft third additional protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30, “the Convention”) by the Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters and the European Committee on Crime Problems.
2. Since the Convention was first established in 1959, criminal activities have become ever-more transnational. International and especially cross-border co-operation is essential to combat transnational crime – and this co-operation should be as rapid, effective, and efficient as possible. At the same time, co-operation and mutual assistance in criminal matters should respect human rights and the rule of law: for Council of Europe member States this includes the standards of protection under the European Convention on Human Rights (ETS No. 5), in particular the right to a fair trial and the right to respect for private life.
3. The Convention has been updated with Protocols approximately every twenty years, with the First Additional Protocol (ETS No. 99) opened for signature in 1978 and the Second Additional Protocol (ETS No. 182) in 2001, to meet the relevant needs of co-operation in criminal matters. The draft third Additional protocol (“the draft third protocol”) follows this pattern: it provides for a welcome modernisation of the Convention by reflecting the use of modern technologies as well as by broadening the range of means via which mutual assistance can be requested and facilitating the execution of mutual assistance requests.
4. The Assembly welcomes that the draft third protocol takes account of modern technological developments to facilitate mutual assistance requests and make them more cost-effective, notably by prioritising secure electronic communication in request procedures, by enabling hearings by video conference (with relevant safeguards), by establishing procedures to facilitate the use of recording devices when the subject of an investigation enters the territory of another Party, as well as a procedure through which Parties can make requests for the interception of telecommunications.
5. As regards hearings by video conference (Article 2), the Assembly notes that Parties may at their discretion apply this possibility to hearings involving the accused person or the suspect. In this case, the manner in which the video conference shall be carried out shall be subject to agreement between the Parties concerned, in accordance with national law and relevant international instruments (Article 2, paragraph 8). The Assembly understands that this should be done in accordance with the right to a fair trial enshrined in Article 6 of the European Convention on Human Rights and/or other similar provisions under international human rights law. This implies that the accused person or suspect should be guaranteed the right to follow the proceedings without technical impediments and the right to legal assistance, including effective and confidential communication with a lawyer. For the sake of clarity, the Assembly proposes that these safeguards be explicitly referred to in the draft explanatory report to the Protocol in relation to Article 2, paragraph 8.
6. A significant part of the draft third protocol (Articles 3 and 4) is designed to facilitate international co-operation concerning State surveillance. The draft text sets out an improved legal basis for such co-operation, with safeguards such as the obligation for the requesting State to indicate the reason why the purpose sought with the surveillance measure cannot be adequately achieved by other means of investigation, thereby facilitating a proportionality test; and the possibility of refusing a request on the ground that such a measure would not have been authorised under the law of the requested Party. The Assembly welcomes these safeguards and notes that they are also meant to cover the refusal of a request on the rule of law or human rights grounds, including on the basis of the European Convention on Human Rights.
7. Whilst supporting the introduction of a legal basis for international co-operation, equipped with sound safeguards, the Assembly recalls that the European Court of Human Rights has identified significant shortcomings in the regulation, oversight and functioning of State surveillance in several member States, in violation of the right to respect for private life guaranteed by Article 8 of the European Convention on Human Rights. Many of these judgments are still pending implementation, indicating that the problems identified by the European Court of Human Rights remain.
8. Along the same lines, in its [Resolution 2513 \(2023\)](#) “Pegasus and similar spyware and secret State surveillance”, the Assembly highlighted the highly intrusive nature of modern spyware used for targeted surveillance, expressing deep concern that spyware had been used illegally or for illegitimate purposes by several member States. The Assembly concluded that recourse to such spyware should be limited to exceptional situations, as a measure of last resort, and always under court supervision.

2. Draft opinion adopted unanimously by the committee on 13 May 2025.

9. Likewise, in its [Recommendation 2258 \(2023\)](#), the Assembly called on the Committee of Ministers to adopt a recommendation to member States of the Council of Europe on secret surveillance and human rights, particularly in the light of the threats posed by new surveillance technologies and spyware; and to examine the feasibility of a Council of Europe convention on the acquisition, use, sale and export of spyware. The Committee of Ministers agreed that a non-binding instrument on secret surveillance and human rights would have a genuine added value and invited the Steering Committee for Human Rights to bear this in mind in its work. In December 2024, the European Commission for Democracy through Law (“Venice Commission”) adopted a report entitled “A rule of law and human rights compliant regulation of spyware” at the request of the Assembly. This concluded that spyware is “an unprecedentedly intrusive surveillance tool”, which should only be developed and used under relevant legal frameworks meeting strict requirements. It transpires from this study that relatively few States have developed legislation that specifically regulates the use of spyware. It is also doubtful whether member States have all the necessary minimum safeguards in place.

10. With these considerations in mind, the Assembly recommends that the draft third protocol be adopted by the Committee of Ministers and opened for signature and ratification. At the same time, however, the Assembly makes a strong call for urgent steps to be taken to ensure that State surveillance is carried out following procedures which are compliant with international standards, failing which greater international co-operation is bound to be flawed. In particular:

10.1. Council of Europe member States should take the necessary steps to implement judgments of the European Court of Human Rights concerning State surveillance by adopting the relevant general measures required;

10.2. Council of Europe member States should ensure that their legal framework for the development and use of spyware includes the minimum safeguards as set out by the Venice Commission;

10.3. the Committee of Ministers should take further steps towards the adoption of a recommendation on secret surveillance and human rights and a legally binding instrument on the acquisition, use, sale, and export of spyware, in light of the Assembly [Recommendation 2258 \(2023\)](#);

10.4. non-member States of the Council of Europe which are Parties to the Convention and wish to become Parties to the Third Additional Protocol should also ensure that their legislative framework on State surveillance and its implementation are compliant with international human rights standards.

B. Explanatory memorandum by Mr Vladimir Vardanyan, rapporteur

1. Introduction

1. The European Convention on Mutual Assistance in Criminal Matters (ETS No. 30, “the Convention”) was opened for signature in 1959 and entered into force in 1962 (). The Convention aimed to enhance co-operation between member States in criminal investigations, evidence gathering, and the prosecution of suspects. At the time of its adoption, a significant part of the Convention focused on the means of co-operation available at the time, notably the use of letters rogatory to request procuring and transferring evidence.

2. Two additional protocols have since updated the Convention. The first of these was opened for signature in 1978 (ETS No. 99). This removed the option provided by the Convention to deny assistance solely on the basis that the request pertains to an offense deemed a fiscal matter by the requested Party. It broadened international co-operation to include the service of documents related to the enforcement of sentences and similar measures. Additionally, it introduced provisions for the exchange of information regarding judicial records. The second protocol was opened for signature in 2001 (ETS No. 182). It was intended to improve responses to cross-border crime in light of social, political, and technological developments, notably by broadening the range of situations in which mutual assistance may be requested and making the provision of assistance easier, quicker, and more flexible.

3. The Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC), operating under the authority of the European Committee on Crime Problems (CDPC), is tasked with reviewing the functioning and implementation of Council of Europe conventions and agreements related to international co-operation in criminal matters, with a view to adapting them and enhancing their practical application as needed.

4. In carrying out its responsibilities, the PC-OC recognised the necessity to update several provisions of the Convention and its Second Additional Protocol, to address recent advancements in practices and support systems for mutual assistance, such as the increased use of video-conferencing and other technological tools. Additionally, it identified areas where practitioners have noted gaps that could be addressed.

5. After considering various approaches, the PC-OC determined that introducing an additional protocol to the Convention would be the most effective and practical solution to modernise it in line with these developments. This proposal received approval from the CDPC, leading to the inclusion of the preparation of a new protocol in the PC-OC's terms of reference for 2022–2025 by the Committee of Ministers.

6. Based on proposals from various delegations, the PC-OC drafted a third additional protocol to the Convention (“the draft third protocol”). This draft was finalised during its 86th meeting (12–14 November 2024) and subsequently submitted to the CDPC for approval. The CDPC reviewed and approved the draft third protocol during its 86th plenary session (20–22 November 2024), forwarding it to the Committee of Ministers for further consideration.

7. On 19 March 2025, at their 1523rd meeting, the Ministers' Deputies agreed to transmit the draft third protocol to the Parliamentary Assembly for opinion. The Committee on Legal Affairs and Human Rights appointed me as rapporteur at its meeting on 7 April 2025.

8. In this explanatory memorandum, I will summarise the previous work of the Assembly on mutual assistance in criminal matters (section 2) and set out the key aspects of the draft third protocol (section 3). I will briefly address the lack of public commentary on the text (section 4), before exploring the issue of State surveillance (section 5). Finally, I will set out some conclusions (section 6).

2. Previous and current work of the Assembly on mutual assistance in criminal matters

9. The Assembly has previously issued Opinions on the original Convention ([Opinion 30](#) (1959)) and on the Second Additional Protocol to the Convention ([Opinion 231](#) (2001)).

10. The Assembly has adopted a number of resolutions and recommendations, which called for improvements in mutual legal assistance in addressing a wide range of criminal issues. These include: [Recommendation 1044](#) (1986) “International crime”; [Resolution 1147](#) (1998) “Threat to Europe from economic crime”; [Recommendation 1507](#) (2001) “Europe's fight against economic and transnational organised crime: progress or retreat?”; [Recommendation 1531](#) (2001) “Security and crime prevention in cities: setting up a European observatory”; [Resolution 1785](#) (2011) and [Recommendation 1953](#) (2011) “The obligation of

member and observer States of the Council of Europe to co-operate in the prosecution of war crimes”; [Resolution 2038 \(2015\)](#) and [Recommendation 2063 \(2015\)](#) “Witness protection as an indispensable tool in the fight against organised crime and terrorism in Europe”, which stressed the need for enhanced mutual assistance in protecting witnesses in cross-border cases; [Resolution 2218 \(2018\)](#) “Fighting organised crime by facilitating the confiscation of illegal assets”; and [Resolution 2279 \(2019\)](#) and [Recommendation 2154 \(2019\)](#) “Laundromats: responding to new challenges in the international fight against organised crime, corruption and money laundering”. It has also adopted a number of texts calling for co-operation and prosecution of international crimes relating to the Russian Federation’s war of aggression against Ukraine, including [Resolution 2436 \(2022\)](#) and [Recommendation 2231 \(2022\)](#) “The Russian Federation’s aggression against Ukraine: ensuring accountability for serious violations of international humanitarian law and other international crimes”, as well as [Resolution 2482 \(2023\)](#), [Resolution 2556 \(2024\)](#) and [Recommendation 2279 \(2024\)](#) “Legal and human rights aspects of the Russian Federation’s aggression against Ukraine”.

3. Main features of the draft third protocol

11. The draft third protocol aims to enhance the capacity of member States and partner States to effectively combat crime. It seeks to achieve this goal by updating and expanding the Convention, along with its two existing Additional Protocols. This purpose is achieved through modernising the current provisions that govern mutual assistance, broadening the scope of means via which mutual assistance can be requested, facilitating assistance and by making it faster and more flexible. By implementing these improvements, the aim of the draft third protocol is to create a more robust framework for international co-operation in criminal matters, enabling States to address contemporary challenges in law enforcement more effectively.

12. The main features of the draft third protocol are as follows:

- article 1 addresses the channels of communication to be used for mutual assistance requests. This article amends Article 15 of the Convention, identifying secure means of electronic communication as the preferred method. The provision further specifies the range of competent authorities which can make particular requests, depending on the subject matter;
- article 2 concerns the use of video conferencing. This article reflects the development of practices which emerged during the covid-19 pandemic. It provides that Parties to the Convention may request that hearings take place by video-conference, in accordance with a set procedure. The requested Party shall agree to such a hearing, provided that the use of the video conference is not contrary to the fundamental principles of its law and that it has the technical means to carry it out. A list of rules is set out, establishing relevant safeguards. Parties may at their discretion facilitate video conferences involving the accused person or the suspect, but only with the agreement of the competent judicial authorities and the individual concerned, in accordance with national law and relevant international instruments. In this context, it is worth noting that the case law of the European Court of Human Rights (“the Court”) on hearings via video link establishes that a defendant’s participation in proceedings by video-conference is not as such contrary to the European Convention on Human Rights (ETS No. 5), but that recourse to this measure in any given case must serve a legitimate aim, and that the arrangements for the giving of evidence must be compatible with the requirements of respect for due process, as laid down in Article 6 of the Convention.³ The Court has held that the defendant must be able to follow the proceedings and to be heard without technical impediments and have effective and confidential communication with a lawyer.⁴ I believe that these safeguards for the accused or suspect should be explicitly mentioned in the draft explanatory report in relation to Article 2, paragraph 8;
- article 3 establishes a framework for the use of technical recording devices that record positions, sound, or images in the territory of another Party. This covers, for example, when the subject of an investigation has a GPS tracker on their vehicle, when an audio recording device has been put in place, or software has been installed on portable electronic devices. When the device is taken to a different jurisdiction, it is beneficial for law enforcement agencies to be able to continue to use the data collected by the device. The article provides that, whenever possible, requests to carry out such surveillance on the territory of another Party should be made in advance. Such requests should provide a set list of information, including the authorising authority of the surveillance, as well as its legal basis, necessity, subject details, implementing measures, and expected duration. Requests may be refused on the grounds that the recording would not have been allowed in a similar domestic case according to the law

3. *Marcello Viola v. Italy*, Application No. 45106/04, judgment of 5 October 2006, paragraph 67.

4. *Grigoryevskikh v. Russia*, Application No. 22/03, judgment of 9 April 2009, paragraph 83.

of the requested Party. The draft explanatory report stipulates that such a refusal may be based on human rights concerns assessed according to the law of the requested Party, in particular as regards the right to respect for private and family life or protection against discrimination on any prohibited ground. Requests may also be refused on the grounds set out in Articles 2 and 5 of the Convention. These grounds include cases where the request concerns an offence which the requested Party considers a political offence, or an offence connected with a political offence; or where the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, public order or other essential interests of its country;

- article 3 also provides for urgent situations where it is not possible to make a request in advance of a technical recording device entering another country. In such cases, the Party using the device shall immediately notify the other Party, providing the same information that is required to make a request in advance. The device may remain active pending authorisation of the notified Party. That notified Party shall, as soon as possible and within ninety-six hours at the latest, indicate whether the device may remain active or whether it validates past activity. In cases where a recording would not have been allowed in a similar domestic case according to the law of the requested Party, the notified Party may decide that the recording may not be carried out or shall be terminated. The procedure also provides the notified Party with a wide range of controls of the activity, including: that any material already recorded while the subject was on its territory may not be used, or that it may be used only under certain conditions; that the continuation or validation of the recording is dependent on the submission of a formal request for mutual assistance; or that the data recorded on its territory should be partially or fully destroyed. The notifying Party may not use the recordings as evidence in criminal proceedings, without explicit authorisation of the notified Party;
- article 3 also provides options for Parties to declare that they will apply certain restrictions to the notification procedure. Such restrictions may include a prohibition on data collection in private homes and places not accessible to the public; and/or limiting authorisation to investigations concerning certain criminal offences;
- article 4 sets out a framework for Parties to request that another Party intercepts telecommunications in the context of criminal investigations. The article requires such requests to include specific information, including a precise description of the telecommunication to be intercepted, relevant technical data, justification for the necessity of the measure, confirmation of authorisation by the requesting Party's competent authority, and the intended duration of the interception. The requested Party may refuse execution, on the same grounds that it may refuse requests made under Article 3. The requested Party may also impose conditions on the execution of requests, such as requiring destruction of irrelevant recorded data, notifying the intercepted individual after the measure, limiting the use of the evidence to the purposes specified in the request, or imposing any other conditions applicable in a similar domestic case. The requesting Party may also ask for transcription, decoding, or decrypting of recordings if necessary, subject to agreement by the requested Party. Judicial authorities in the requested Party may destroy parts of the records deemed irrelevant or covered by legal privilege before transmitting them to the requesting Party. If the intercepted communication reveals that an offence was committed wholly or mainly within the territory of the requested Party, the requesting Party is encouraged to consider transferring information to enable prosecution in that jurisdiction;
- article 5 of the draft third protocol sets out rules as to the payment of costs involved in the provision of mutual assistance. It sets out a list of particular costs that will be refunded by the requesting Party, unless the Parties agree otherwise. Other than this, the article provides that Parties shall not claim from each other the refund of any costs resulting from the application of the Convention or its Protocols, except for costs incurred by attendance of experts in the territory of the requested Party; costs incurred by the transfer of a person in custody; and costs of a substantial or extraordinary nature. Article 5 is exactly the same as a similar provision in the Second Protocol to the Convention, except for one change. The list of particular costs that will be refunded by the requesting Party has been expanded, to include "the costs which are incurred by telecommunications operators or service providers in executing requests for the interception of telecommunications, as well as the costs arising from the transcription, decoding and decrypting of the intercepted communications when applicable";
- article 6 addresses the issue of timely execution of mutual assistance requests in criminal matters. It establishes a general principle that such requests should be handled with the same celerity and priority as comparable domestic cases. The article recognises that certain circumstances, such as procedural deadlines, the gravity of the offence, or other urgent matters, may necessitate setting specific time limits for execution. In such cases, the requested Party should make every effort to meet these deadlines, to

the extent that this is possible. When the requested Party cannot meet a specified time limit, it must promptly inform the requesting Party through any available means, after which the Parties may consult on appropriate timing and conditions;

- article 7 addresses data protection, replacing Article 26 of the Second Additional Protocol. It provides that personal data transferred as a result of the execution of a request made under the Convention or its Protocols may only be used by the receiving Party for the purpose of proceedings to which the Convention or any of its Protocols apply; for judicial or administrative proceedings which are directly linked; or for preventing an immediate and serious threat to public security. Data may be used for other purposes, if prior consent is provided by either the transferring Party or the data subject. Parties may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or its Protocols where such data are protected under their national legislation, and/or when the receiving Party is not bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as modernised by the Protocol amending this Convention (CETS No. 223), unless the receiving Party undertakes to afford such protection to the data as is required by the transferring Party. Any Party that transfers personal data obtained as a result of a request made under the Convention or its Protocols may require the receiving Party to provide information of the use made of the data. Finally, any Party may, by a declaration, require that, within the framework of procedures for which it could have refused or limited the transmission or the use of personal data in accordance with the provisions of the Convention or one of its Protocols, personal data which it transmits to another Party not be used by the latter unless with its previous consent;
- the remaining articles of the draft third protocol provide for: the friendly settlement of difficulties regarding the interpretation of the Convention and its protocols (Article 8); a summary of how the provisions of the draft third protocol relate to existing provisions in the Convention and its Additional Protocols (Article 9); principles governing the Parties' signature of the Protocol and its entry into force (Article 10); accession to the Protocol (Article 11); its territorial application (Article 12); reservations and declarations (Article 13); denunciation (Article 14); and notifications (Article 15). Articles 10 to 15 are based on the "Model final clauses for Conventions, Additional Protocols and Amending Protocols concluded within the Council of Europe" adopted by the Committee of Ministers on 5 July 2017, and the final clauses of the Convention;
- article 13 provides that the only reservations possible in relation to the draft third protocol are for Article 3 and 4. Parties may avail themselves of the right not to accept either one or both of these articles, either wholly or in part.

4. Positions voiced by different stakeholders

13. There were no representatives of legal associations or other non-governmental organisations present in any of the PC-OC meetings during which the draft third protocol was prepared. It is noteworthy that no civil society organisations attended the drafting process of the draft third protocol – and there has been no public commentary about the text. In this context, there is a shortage of information and analysis about the important questions reflected in the draft protocol including issues surrounding the use of State surveillance.

5. The issue of State surveillance

14. The draft third protocol impacts an issue affecting fundamental rights that the Assembly has been particularly concerned with in recent years: the use of spyware and other means of State surveillance.

5.1. Judgments of the European Court of Human Rights

15. The European Court of Human Rights has issued many judgments on the wider issue of State surveillance, identifying practices which are incompatible with Article 8 of the European Convention on Human Rights. Most concerningly, many of these judgments are still pending implementation, meaning that the Committee of Ministers of the Council of Europe has not yet been provided with sufficient evidence to demonstrate that the problem(s) which caused the human rights violation(s) has been resolved. Judgments still pending implementation include those identifying a lack of sufficient safeguards against abuse in the use of secret surveillance (*Ekimdzhev and Others v. Bulgaria*,⁵ *Zoltan Varga v. Slovakia*,⁶ *Bucur and Toma*

5. Application No. 70078/12, judgment of 11 January 2022.

6. Application No. 58361/12, judgment of 20 July 2021.

v. Romania,⁷ *Iordachi and Others v. the Republic of Moldova*,⁸ and *Pietrzak and Bychawska-Siniarska and Others v. Poland*⁹), inadequate reasoning in the decisions of domestic courts authorising surveillance measures (*Simic v. Serbia*,¹⁰ *Potoczka and Adamco v. Slovakia*¹¹), the impossibility of third parties in criminal proceedings to challenge telephone tapping warrants (*Contrada v. Italy (No.4)*,¹² *Pruteanu v. Romania*¹³), and the unjustified interception of lawyers' telephone data (*Bersheda and Rybolovlev v. Monaco*¹⁴).

5.2. Spyware – findings and work of Council of Europe bodies

16. The European Court of Human Rights has not yet issued judgments on the use of spyware. However, this has been a subject of great concern to the Assembly and the European Commission for Democracy through Law (Venice Commission).

17. In [Resolution 2513 \(2023\)](#) “Pegasus and similar spyware and secret State surveillance”, the Assembly noted how investigative reports had concluded that many Council of Europe member States have acquired and used Pegasus for targeted surveillance. Others have acquired or used similar spyware, such as Candiru and Predator. Spyware can be extremely intrusive, granting the user complete and unrestricted access to all sensors and information on the targeted device. It turns the smartphone into a 24-hour surveillance device, accessing the camera and microphone, geolocation data, e-mails, messages, photos, videos, passwords and applications. The Assembly expressed deep concern that spyware have been used illegally or for illegitimate purposes by several member States, including against journalists, political opponents, and human rights defenders. Secret surveillance of political opponents, public officials, journalists, human rights defenders and civil society actors for purposes other than those exhaustively enumerated in Article 8.2 of the European Convention on Human Rights amounts to a clear violation of the right to respect for private life (Article 8).

18. The Assembly concluded that the use of such spyware should be limited to exceptional situations, as a measure of last resort, to prevent or investigate a specific act amounting to a genuine and serious threat to national security or a specific and precisely defined serious crime, targeting only the person suspected of committing or planning to commit those acts, and always under court supervision. In order to limit such a high level of intrusiveness, States should take into account the proportionality of new spyware before acquiring and using it; they should also consider using spyware without some of the most invasive features of Pegasus or a version that is programmed in such a way that it limits access to what is strictly necessary.

19. The Assembly called on member States which seem to have acquired or used Pegasus, including Germany, Belgium, Luxembourg and the Netherlands, to clarify the framework of its use and applicable oversight mechanisms. It invited them to send this information, as well as any statistics on the use of Pegasus, to the Assembly and the Venice Commission within three months. The Assembly also asked the Venice Commission to assess the legislative framework and practice on targeted surveillance of all member States, in order to assess if the framework contains adequate and effective guarantees against any possible abuse of spyware.

20. In [Recommendation 2258 \(2023\)](#), the Assembly called on the Committee of Ministers to adopt a recommendation to member States of the Council of Europe on secret surveillance and human rights, particularly in the light of the threats posed by new surveillance technologies and spyware; to examine the feasibility of a Council of Europe convention on the acquisition, use, sale and export of spyware; and to co-ordinate its efforts with other international organisations for the purposes of standard setting and co-operation. In its reply to the Assembly's recommendation of 4 September 2024 ([Doc. 16030](#)), the Committee of Ministers indicated that a recommendation on secret surveillance and human rights would be feasible and have genuine added value – and invited the Steering Committee for Human Rights (CDDH) to bear this in mind for the mid-term review of its terms of reference. In November 2024, the CDDH decided to request the Committee of Ministers to give it terms of reference to prepare a non-binding instrument on human rights, the use of spyware, and secret State surveillance.¹⁵

7. Application No. 40238/02, judgment of 8 January 2013.
8. Application No. 25198/02, judgment of 10 February 2009.
9. Application No. 72038/17 and 25237/18, judgment of 28 May 2024.
10. Application No. 9172/21, judgment of 14 January 2025.
11. Application No. 7286/16, judgment of 12 January 2023.
12. Application No. 2507/19, judgment of 23 May 2024.
13. Application No. 30181/05, judgment of 3 February 2015.
14. Application No. 36559/19, judgment of 6 June 2024.
15. CDDH(2024)R101.

21. The Venice Commission adopted a report in December 2024, entitled “A rule of law and human rights compliant regulation of spyware”, at the request of the Assembly. This concluded that spyware is “an unprecedentedly intrusive surveillance tool” and that it is “crucial to provide for clear contours concerning the use of spyware by State in order to prevent and eradicate abusive practices”. The Venice Commission found that the development and use of spyware should only be possible if the relevant legal framework meets certain requirements, setting out an 11-point list of minimum safeguards which includes the following. The use of spyware must be regulated by primary legislation, which should clearly define the (restricted) scope *ratione materiae*, *personae* and *temporis* of targeted surveillance through spyware. The requesting authorities (law enforcement or intelligence agency) should always demonstrate that the information sought in the investigation was necessary to the legitimate purpose and could not be obtained by less intrusive means. There must be well-regulated *ex-ante* authorisation procedures before a court or another independent body; and the duration of the surveillance measures must be limited to what is strictly necessary. The whole surveillance process needs to be backed up by effective external independent oversight institutions, which are sufficiently resourced, qualified and specialised, and cannot be entrusted exclusively to the executive. The persons under surveillance must be notified subsequently, subject to exceptions defined by law, so that they can be involved in monitoring and challenging the measure.¹⁶

22. Although the Venice Commission did not make an individual assessment of whether the legislative framework of each member State complies with all minimum safeguards, it transpires from the report that many member States do not yet have all these safeguards in place. In fact, relatively few States have developed legislation specifically regulating the use of spyware. The Assembly will remain seized of this important matter, including through the follow-up work of Pieter Omtzigt (Netherlands, EPP/CD), rapporteur for follow-up to Resolution 2513 (2023) “Pegasus and similar spyware and secret State surveillance”, for the Committee on Legal Affairs and Human Rights.

5.3. State surveillance – contents of the draft third protocol

23. Many of the key provisions of the draft third protocol have the effect of establishing new procedures for Parties to co-operate to carry out electronic surveillance. Article 3 establishes a procedure to facilitate continued surveillance where one Party has initiated electronic surveillance of a subject and that subject moves to the territory of another Party. Article 4 establishes a procedure where one Party can request that another intercepts the telecommunications of a subject. Article 5 establishes that the costs of intercepting telecommunications will be reimbursed by the Party that requested the interception.

24. Spyware is not mentioned explicitly in any of these provisions, but according to the draft explanatory report, Article 3 is meant to cover the continued use of software installed on portable electronic devices in the territory of another Party. Spyware would clearly fall within the scope of this provision.

25. It is very important that law enforcement agencies are able to carry out surveillance in cross-border situations – as long as this is done only in appropriate cases and with proper safeguards.

26. There are some reasons to conclude that the draft third protocol increases the procedural guarantees governing electronic surveillance. This is because, mutual legal assistance requests for cross-border electronic surveillance are already possible under the existing Convention and its protocols. The provisions of the draft third protocol establish procedures that are specifically tailored to the use of electronic surveillance and that provide for additional safeguards. In particular, Article 3 (on the use of technical recording devices in the territory of another Party) and Article 4 (on requests for interception of telecommunications) have particular safeguarding features. The first is that Parties to the Protocol may choose not to accept either of these Articles, either wholly or in part. The second is that, in relation to Article 3, Parties may declare that the notification procedure cannot be used for the collection of data in private homes and places; and/or that the notification procedure can only be used for a limited list of offences.¹⁷ Third, under both Article 3 and Article 4, the requesting States need to justify that the measures were ordered lawfully and why the purpose sought with the use of the technical recording device or the interception of telecommunications cannot be adequately achieved by less intrusive measures, i.e. that surveillance is used as a measure of last resort. Fourth, both

16. Venice Commission, “A rule of law and human rights compliant regulation of spyware”, 13 December 2024.

17. The offences referred to are those listed in Article 17, paragraph 7 of the Second Additional Protocol to the Convention, namely: assassination, murder, rape, arson, counterfeiting, armed robbery and receiving of stolen goods, extortion, kidnapping and hostage taking, traffic in human beings, illicit traffic in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, use of explosives, illicit carriage of toxic and dangerous waste, smuggling of aliens, sexual abuse of children.

Article 3 and Article 4 establish a safeguard which is not present in relation to other subjects of mutual legal assistance requests in most cases, which is that Parties may choose to refuse a request when the same request would not have been accepted in a similar domestic case according to the law of the notified Party.

27. In this way, there are indications that the draft third protocol introduces a greater range of reasons for a Party to refuse to allow electronic surveillance in its territory: either because it has declared that it will not accept mutual assistance requests in such cases; or by deciding that such a request should be refused, through the application of its own domestic law to the circumstances of the case (including on grounds that it is incompatible with human rights standards), which is not possible for other subjects of mutual assistance requests.

28. It is also important to note that the draft third protocol will have no impact on the actions of States conducting clandestine or intelligence operations. It will only be relied upon by States when they are engaged in a criminal procedure. Therefore, by establishing an additional procedure for technological surveillance, which has additional safeguards that were not present before, the draft third protocol may expose such surveillance to additional examination.

29. At the same time, the very adoption of the draft third protocol also raises some concerns – not because of the provisions of the draft third protocol itself, but because of the general context of the regulation of State surveillance in Europe. As set out above, there are widespread and significant shortcomings in the regulation of State surveillance as a whole (as indicated by judgments of the European Court of Human Rights which are still pending implementation), and the use of spyware in particular (as indicated by reports of the Assembly and opinions of the Venice Commission). The draft third protocol formalises a legal procedure for the use of State surveillance in cross-border contexts. Council of Europe member States are therefore institutionalising co-operation for State surveillance, at a time when most States have demonstrably inadequate regulation of it. This should serve as a timely reminder of the need for States to redouble their efforts to ensure there are adequate safeguards for the use of State surveillance – not only in their own countries, but also in the countries that they are co-operating with in criminal matters.

6. Conclusions

30. The constant movement of individuals across borders, as well as the transnational nature of criminal activities and organisations, means that States cannot fight crime effectively without co-operating with each other. It is essential that this co-operation is as efficient and effective as possible, whilst retaining the necessary safeguards to protect fundamental rights. The Convention was first created in 1959 and has been updated with additional Protocols roughly every two decades: firstly in 1978, secondly in 2001, and thirdly now in 2025. The Assembly should welcome this work to modernise the Convention to reflect the use of modern technology.

31. The draft third protocol does this by identifying secure electronic communications as the preferred way of transmitting mutual assistance requests in criminal matters; formalising and facilitating the use of video conferencing for hearings; establishing frameworks for the use of electronic recording devices in the territory of other States; and formalising a system by which one Party can request another to intercept electronic communications in its territory. These are all welcome and important steps to ensuring timely and effective co-operation in criminal matters.

32. The draft third protocol provides an improved legal basis for international co-operation to facilitate State surveillance, with relevant safeguards. At the same time, given a context where there is inadequate regulation of State surveillance in many European States – particularly for spyware – the adoption of the draft third protocol should be a wake-up call for the need for new efforts by States to ensure better regulation of State surveillance.

33. In light of these concerns, I suggest that the Assembly welcomes the draft third protocol, whilst emphasising that it must be accompanied by renewed efforts to ensure that State surveillance is carried out in an appropriate manner. This includes the full and timely implementation of judgments of the European Court of Human Rights, the adoption of legal frameworks for the development and use of spyware that include the minimum safeguards set out by the Venice Commission, the adoption of a recommendation on secret surveillance and human rights, and the elaboration of a legally binding Council of Europe instrument on the acquisition, use, sale and export of spyware.