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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15379
28 September 2021

Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Kamal JAFAROV, Azerbaijan, European Conservatives Group and Democratic Alliance

Summary

The Committee on Legal Affairs and Human Rights welcomes the success that the Convention on Cybercrime (ETS No. 185) is enjoying world-wide, with 66 ratifications. It notes that since the adoption of the Convention in 2001, the exploitation of information technology for criminal purposes has strongly increased. Cybercrime is considered by many States as a serious threat to human rights, the rule of law, and to the functioning of democratic societies and even to national security.

The purpose of the Second Additional Protocol to the Convention on Cybercrime is to provide sharper tools to investigate cybercrime and obtain justice for victims. The Draft Protocol is designed to function within the criminal justice systems of the Parties with all the procedures, regulations, methods for transmitting data, conditions and safeguards foreseen in the respective national legal systems.

The Convention on Cybercrime and its Additional Protocols face a dilemma. The purpose of these treaties presupposes that as many States as possible participate in fighting cybercrime as the latter does not recognise borders. But States' legal systems differ, also in the spheres of criminal law and data protection. The Convention and its Protocols can therefore only set minimum standards of protection that must be implemented by all participant States whilst leaving open the possibility for more advanced States to implement stronger protections. But such higher standards of protection must not jeopardise the common goal of the Convention and its Protocols, namely, to make international co-operation in the fight against cybercrime more efficient and effective.

The committee considers that the Second Additional Protocol in principle strikes a reasonable balance. Having considered numerous proposals by different stakeholders, it suggests nevertheless some improvements to further strengthen the protection of human rights.

1. Reference to committee: Doc. 15316, Reference 4593 of 21 June 2021.

Contents **Page**

A. Draft opinion[2]

1. The Parliamentary Assembly recalls that the 20th anniversary of the adoption of the Convention on Cybercrime (ETS No. 185) will be celebrated in November 2021. It welcomes the success that this Convention of the Council of Europe is enjoying world-wide, currently with 66 ratifications.

2. The Assembly notes that since 2001, the exploitation of information technology for criminal purposes has strongly increased. Cybercrime is considered by many States as a serious threat to human rights, the rule of law, and to the functioning of democratic societies and even to national security. Examples of cybercrimes include online sexual violence against children, the theft and misuse of personal data, election interference and other attacks against democratic institutions, attacks against critical State and public service infrastructures, misuse of informational technology for terrorist purposes and during the ongoing Covid-19 pandemic, cyberattacks on hospitals and laboratories developing vaccines, misuse of domain names to promote fake vaccines and treatments, etc.

3. The purpose of the Second Additional Protocol to the Cybercrime Convention is to provide sharper tools to investigate cybercrime and obtain justice for victims. Given the prevalence of cybercrime today, victims of online crime must be given a better chance at obtaining justice, and perpetrators must be made to face a substantially greater risk of being held to account.

4. The Assembly recalls its previous work on the fight against cybercrime, including its Opinion 226 (2001) "Draft Convention on cyber-crime", its Opinion 240 (2002) "Draft additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", its Recommendations 2041 (2014) "Improving user protection and security in cyberspace" and 2077 (2015) "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet" and most recently, its Resolution 2256 (2019) ″Internet governance and human rights″. The Assembly has consistently taken a constructive approach to improving international co-operation in this field whilst upholding human rights.

5. The Assembly recognises that the Draft Protocol is designed to function within the criminal justice systems of the Parties with all the procedures, regulations, methods for transmitting data, conditions and safeguards foreseen in the respective national legal systems. This applies also to the ″direct co-operation″ provided for by Articles 6 and 7, both of which require Parties to establish a proper domestic legal basis for the exercise of these powers.

6. The Assembly further recognises that both the Cybercrime Convention itself and its Additional Protocols face a difficult dilemma. The purpose of these treaties presupposes that as many States as possible to participate in fighting cybercrime as the latter does not recognise borders. Otherwise, cybercriminals will continue to operate from safe havens, to the detriment of their victims all over the world. Countries have very different legal systems, including in the sphere of criminal law and different levels of regulation regarding data protection. The Convention and its Protocols can therefore only set minimum standards of protection that must be implemented by all participant States whilst leaving open the possibility for more advanced States to implement stronger protections for their citizens. But such higher standards of protection must not jeopardize the common goal of the Convention and its Protocols, namely, to make international co-operation in the fight against cybercrime more efficient and effective.

7. The Assembly considers that the Second Additional Protocol to the Cybercrime Convention in principle strikes a reasonable balance in facing the dilemma described above. Having considered numerous proposals by different stakeholders, it suggests nevertheless the following improvements to further strengthen the protection of human rights, in particular the right to privacy:

7.1. enshrine the application of the principle of proportionality in the text of Article 13, in addition to this being mentioned in the Draft Protocol's explanatory report;

7.2. specify in Article 14 paragraph 2 that the further processing of personal data by the receiving Party shall be provided by law, and shall constitute a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest or shall otherwise provide for the adequate protection of human rights and liberties;

7.3. include in the list of information to be made available to data subjects under Article 14 paragraph 11 the contact details of the competent data controller;

2. Draft opinion adopted unanimously by the committee on 27 September 2021.

7.4. update paragraph 12 (b) of the Draft Protocol so as to ensure that as a general rule, information to individuals related to access and rectification shall be provided free of charge;

7.5. expressly recognise in the text of the Draft Protocol or its explanatory report that privileges and immunities of certain professions such as lawyers, doctors, journalists, religious ministers, or parliamentarians shall be respected;

7.6. make mandatory the public disclosure, by oversight authorities, of aggregate information on the use of the measures under the Protocol and on the number of individuals affected by them;

7.7. in the provisions allowing evidence taking by video conferencing, to accommodate witness protection measures available at national level; and to include the possibility for lawyers to participate in a hearing conducted by video conference to be able to defend their clients' interests;

7.8. to enhance ″equality of arms″ between prosecution and defence by compelling the competent authorities of the Parties to make use of the investigative instruments placed at their disposal by the Draft Protocol also on behalf of the defence.

B. Explanatory memorandum by Mr Kamal Jafarov, rapporteur

1. Context

1. The Convention on Cybercrime (ETS No. 185, also known as ″Budapest Convention″ or ″Cybercrime Convention″) was opened for signature in 2001 and has since then attracted membership from all regions of the world (66 ratifications as of June 2021). The United States of America are a State party to the Convention but not to its (first) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). This issue was omitted from the original Cybercrime Convention in order to enable the United States to join, despite their far-reaching constitutional protection of freedom of speech. The Russian Federation is the only Council of Europe member State that has neither signed nor ratified the Cybercrime Convention; Ireland has signed but not ratified it.

2. Since 2001, the use of information technology for criminal purposes has strongly increased. Cybercrime is considered by many States as a serious threat to human rights, the rule of law and to the functioning of democratic societies and even to national security. The explanatory report on the Draft Second Additional Protocol gives numerous examples of such threats, including online sexual violence against children, the theft and misuse of personal data (″identity theft″), election interference and other attacks against democratic institutions, attacks against critical infrastructures (including ″denial of service″ or ″ransomware attacks″), the misuse of such technology for terrorist purposes, etc. During the ongoing Covid-19 pandemic, States observed related cybercrime such as attacks on hospitals and laboratories developing vaccines and the misuse of domain names to promote fake vaccines and treatments.

3. Both the Cybercrime Convention itself and its additional Protocols, including the Draft Second Additional Protocol, which is the subject of this Opinion,[3] have to face a difficult dilemma. The purpose of the Convention and its Protocols requires that as many States as possible participate, as cybercrime does not recognise borders. Otherwise, cybercriminals will continue to operate from safe havens, to the detriment of their victims all over the world. Countries have very different legal systems, including in the sphere of criminal law and – why not admit it – different levels of awareness and regulation regarding data protection. This means that the Convention and its Protocols can only set minimum standards of protection that must be implemented by all participant States whilst leaving open the possibility of more advanced States to implement stronger protections for their citizens. But such higher standards of protection must not jeopardise the common goal of the Convention and its Protocols, and in particular the Draft Second Additional Protocol, namely, to make international co-operation in the fight against cybercrime more efficient and effective. In my view, the drafters of the Second Additional Protocol have succeeded in principle to strike a reasonable balance between various interests at stake while facing the aforementioned dilemma. Having considered numerous proposals by different stakeholders, I suggest nevertheless some amendments to the Draft Protocol to further strengthen the protection of human rights, in particular the right to privacy (see below, chapter 5).

2. Previous work of the Assembly

4. The Assembly's previous work on the topic of the fight against cybercrime shows that its position has always been in favour of strong measures against cybercrime whilst maintaining the highest possible level of protection for the internet users' privacy rights.

5. In its Opinion on the Draft Convention on Cybercrime (Opinion 226 (2001)), the Assembly considered ″the fight against cybercrime to be a crucially important challenge in view of the obstacles which this form of crime may pose to the development of new technologies″ (paragraph 1) and noted *inter alia* that ″it is essential that there be common definitions of criminal offenses, that the private sector continue to work on rendering computer networks secure; that governments issue appropriate and proportionate domestic legislation″ (paragraph 4). In its numerous proposals for amendments, the Opinion stressed the need for even stronger protection of privacy rights and for the speedy negotiation of a Protocol covering ″new forms of offence″ such as the dissemination of racist propaganda, abusive storage of hateful messages, the use of the internet for trafficking in human beings and the obstruction of the functioning of computer systems by ″spamming″. In his explanatory report, the Rapporteur stressed the ″unconditional rejection of a 'cyber-police' operating irrespective of national boundaries and sovereignty. Any idea of a 'cyber police force' going beyond the framework of individual nations and their sovereign responsibilities must implicitly be ruled out. […] For

3. See Doc. 15316rev.

example, while any country may conduct an investigation on behalf of another, there can be no transfrontier enquiries or searches. Contrary to the fears that have been expressed, therefore, the Draft convention does not contemplate remote searches. This attitude is at variance with that of the United States, which believes that specialist internet investigators must enjoy freedoms commensurate with the international nature of the World Wide Web." Subsequent developments have shown that the tools provided in the original Convention were not sufficient to cope with the dramatic increase in cybercrime – hence the negotiation of the Second Additional Protocol.

6. In its Opinion on the Draft (first) additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Opinion 240 (2002)), the Assembly "realises that the text adopted by the European Committee on Crime Problems is a compromise between differing legal and cultural traditions, which strikes a broadly satisfactory balance between combating racism and freedom of expression." (paragraph 4) The Assembly's most important amendment proposal was to add the notion of "unlawful hosting". This proposal was not implemented in the final draft.

7. In its Recommendation 2041 (2014) "Improving user protection and security in cyberspace", the Assembly invited the Committee of Ministers to consider the feasibility of drafting an additional Protocol to the Cybercrime Convention regarding serious violations of fundamental rights of users of online services; and to analyse to what extent the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) needed to be updated in order to deal with mutual assistance concerning transnational cybercrime and cyber evidence. It also invited the Committee of Ministers, on the basis of evidence released by Edward Snowden about mass violations of the right to privacy under Article 8 of the European Convention on Human Rights (ETS N° 5), to set up an action plan to prevent such violations (paragraphs 2.1, 2.2 and 2.9).

8. In its Recommendation 2077 (2015) "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet", the Assembly recommended that the Committee of Ministers invites the Parties to the Cybercrime Convention and to its Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems to study the feasibility of drafting additional Protocols defining a common level of criminalisation of large-scale cyberattacks, including minimum standards for penalties; on mutual assistance regarding investigative powers, extending in particular the scope and application of Article 32 of the Convention; and on criminal justice access to data on cloud servers. The Assembly also called on the Committee of Ministers to draft legal standards on the international responsibility of States for taking all reasonable measures to prevent large-scale cyberattacks from being launched by persons under their jurisdiction or emanating from their national territory against computer systems in another State. (paragraphs 3.1.-3.3.).

9. Most recently, in its Resolution 2256 (2019) "Internet governance and human rights", the Assembly reiterated the need to ensure more effective protection of human rights on the internet. Whilst underlining the need to guarantee the effective protection of freedom of expression and information online and offline, it stressed that more must be done to counteract the dangers brought about by abuses of these rights, such as incitement to discrimination, hatred and violence, including terrorism, child sexual abuse, online bullying, the manipulation of information and propaganda. This requirement is connected with the need to ensure that the internet becomes a secure environment in which users are protected from arbitrary action, threats, attacks on the physical and mental integrity and violations of their rights. The Assembly once more underlined the threat to human rights posed by the large-scale systems set up by intelligence services for the mass collection, preservation, and analysis of communications data. The Assembly therefore recommended to the Council of Europe's member States to "consider holistic policies for combating computer crime […], including the setting-up of police forces specialised in detecting and identifying online criminals and equipped with appropriate technical resources […]." (paragraphs 5-7, 9.3.) Regarding the Cybercrime Convention, the Assembly considered that it should be better used to enhance interstate collaboration and called on those member States, which had not yet done so to ratify it; and it supported the completion of the negotiations on the second additional Protocol on enhanced international co-operation and access to evidence of criminal activities in the cloud. (paragraph 11)

3. Main features of the Draft Second Additional Protocol

10. **Chapter II** of the Draft Second Additional Protocol ("the Draft Protocol" or "the Protocol") foresees several "measures for enhanced co-operation", including, in **Section 2**, "Procedures enhancing direct co-operation with providers and entities in other Parties." Concretely, Article 6 enables competent authorities to directly request from service providers resident in another State Party domain name registration information, and under Article 7 the disclosure of subscriber information. **Section 3** on "Procedures enhancing

international co-operation between authorities for the disclosure of stored computer data" foresees giving effect to orders from another Party for expedited production of data (Article 8) and the expedited disclosure of data in an emergency (Article 9). **Section 4** (Article 10) lays down "Procedures pertaining to emergency mutual assistance". Finally, **Section 5** on "Procedures pertaining to international co-operation in the absence of applicable international agreements" allows for video conferencing (Article 11), and, importantly, joint investigation teams (JITs) and joint investigations (Article 12).

11. **Chapter III** deals with conditions and safeguards (Article 13), in particular for the protection of personal data (Article 14). This chapter, together with Section 2 on direct co-operation with service providers, is the main focus of criticisms by civil society.

4. Criticism and recommendations voiced by different stakeholders

12. The European Data Protection Board (EDPB),[4] in its contribution dated 4 May 2021[5] criticises the short deadline for comments on the first complete draft of the Protocol published on 14 April 2021. It stresses the need for further assessment of the draft provisions on data protection, in particular as to their compatibility with the General Data Protection Regulation (GDPR) and the case law of the Court of Justice of the European Union (CJEU). On substance, the EDPB recommends that the drafters shall:

– clarify the binding nature of the data protection safeguards in the Draft Protocol;

– ensure the systematic involvement of a judicial or an independent administrative authority in the requested parties, except in cases of validly established urgency, also to implement the dual criminality principle, in line with CJEU case law;

– clarify the definition of subscriber information in order to avoid inclusion of any traffic or content data;

– develop further specifications and requirements regarding security and authentication of the bodies empowered to request and receive data;

– enshrine the application of the principle of proportionality in the text of Article 13;

– clarify in Article 14 that the Draft Protocol applies to Parties, unless another agreement or arrangement between the concerned Parties provides the same or higher level of protection regarding privacy and the protection of personal data than the Protocol itself;

– clarify in Article 14 paragraph 1(a) that personal data received by requested authorities or private entities as included in the request shall be protected in the same way as the personal data received by the requesting authorities;

– allow the Party transferring personal data (within a request or in a reply to a request) to require from the receiving Party additional safeguards or to allow the requested Party to refuse such transfer so as to ensure that the level of protection of personal data under European Union law is not undermined;

– specify in Article 14 paragraph 2 that the further processing of personal data by the receiving Party should be provided by law, and should constitute a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest;

– replace, in Article 14 paragraph 4, the words "considered sensitive in view of the risks involved" by "which allow or confirm the unique identification of that natural person";

– in Article 14 paragraph 6, concerning automated decisions, clarify that in addition to human intervention, safeguards under domestic law of the Parties authorising such processing shall provide guarantees for the rights and freedoms of the data subject; and to include in paragraph 6 a specific provision prohibiting the processing of sensitive data for the purpose of automated decision making, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are explicitly mandated for under paragraph 6;

---

4. The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes co-operation between the EU's data protection authorities. It is established by the General Data Protection Regulation (GDPR) and is based in Brussels. The EDPB is composed of representatives of the EU national data protection authorities (National Supervisory Authorities), and the European Data Protection Supervisor (EDPS). (Who we are | European Data Protection Board (europa.eu)).

5. EDPB contribution to the 6th round of consultations on the Draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime, Brussels, 4 May 2021 (in English only).

– explicitly extend the application of Article 14 paragraph 8 (on maintaining records) to any processing activities and in particular to ″storage″;

– include in the list of information to be made available to data subjects under Article 14 paragraph 11 the contact details of the competent data controller;

– complement the provisions under Article 14 paragraph 12 in order to ensure that any individual may seek and obtain information as to whether or not personal data concerning him or her are being processed; as a general rule, information to individuals related to access and rectification shall be provided free of charge, as an update of paragraph 12(b); and the conditions under which information and data subject rights may be restricted should be clarified and specified in order to be fully consistent with EU law, and notably meet the foreseeability and proportionality criteria;

– ensure the respect of safeguards attached to personal data such as privileges and immunities of certain professions;

– clarify Article 14 paragraph 13 on effective remedies so as to ensure that both judicial and non-judicial remedies are available under the jurisdiction of each Party to the Cybercrime Convention to any concerned data subjects.

13. The European Union's Fundamental Rights Agency (FRA) has welcomed the Draft Protocol in principle:

"The Draft replies to the need to establish a clear, foreseeable and operational legal framework, supporting both international co-operation on cybercrime and the collection of e-evidence related to a criminal offence for criminal investigations and proceedings. The Draft Second Additional Protocol sets up legal boundaries, paying specific attention to fundamental rights, and notably the right to the protection of personal data."

14. The FRA nevertheless makes some suggestions for further improvements, in particular:

– in Article 11 paragraphs 1 and 5, to stress the *ne bis in idem* principle, to avoid double penalisation of a witness in case of perjury or similar offenses, if both States administered the oaths or other warnings;

– in Article 11 paragraph 7 on video conferencing, to accommodate witness protection measures available at national level (for example face or voice distortion);

– in Articles 7 paragraph 1 and 8 paragraph 1, to enhance ″equality of arms″ between prosecution and defence by foreseeing that at national level, the Contracting Parties' competent authorities may also act on behalf of the defence;

– in Article 7 paragraphs 7 and 8 and in Article 8, to further clarify the reasons for which a service provider may lawfully refuse to disclose subscriber information; violations of fundamental rights in the requesting or requested State should be recognised as such a reason.

15. Civil society groups have also reacted strongly to the publication of the Draft Protocol. Regarding the procedure followed by the drafting committee (T-CY), the Electronic Frontier Foundation sums up the criticism by civil society as follows:

"In 2018, nearly 100 public interest groups called on the CoE to allow for expert civil society input on the Protocol's development. In 2019, the European Data Protection Board (EDPB) similarly called on T-CY to ensure "early and more proactive involvement of data protection authorities" in the drafting process, a call it felt the need to reiterate earlier this year. And when presenting the Protocol's draft text for final public comment, T-CY provided only 2.5 weeks, a timeframe that the EDPB noted "does not allow for a timely and in-depth analysis" from stakeholders. That version of the Protocol also failed to include the explanatory text for the data protection safeguards, which was only published later, in the final version of May 28, without public consultation. Even other branches of the CoE, such as its data protection committee, have found it difficult to provide meaningful input under these conditions."[6]

16. On substance, a collective of internet freedom groups[7] strongly criticised the Draft Protocol a joint letter to the President of the Assembly, Rik Daems, and other Council of Europe bodies dated 2 May 2021. The undersigned see a threat to the rule of law in that Section 2 permits ″direct co-operation″ with private entities,

6. See Global Law Enforcement Convention Weakens Privacy & Human Rights | Electronic Frontier Foundation (eff.org), 8 June 2021.

7. Electronic Frontier Foundation, European Digital Rights, IT-Pol Denmark, AI Sur, Article 19, Derechos Digitales and Homo Digitalis, Access Now, dataskyyd.net, Digital Rights Ireland, Digitale Gesellschaft, Fundacion Karisma, IPANDETEC Centroamerica, Vrijschrift.org.

thereby encouraging the voluntary disclosure of personal data such as domain name registration information and subscriber information without mandatory judicial authorisation for all production orders under the Protocol. They also criticised a lack of safeguards against ″re-purposing″ of data once received under the Protocol and against ″forum shopping″ in joint investigations as well as a lack of transparency. The undersigned therefore recommend, *inter alia*, that:

– judicial authorisation should be mandatory for all production orders under the Protocol, including those under Article 6 (request for domain name registration information);

– Parties to the Additional Protocol should be required to accede to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223, "Convention 108+");

– the Protocol should provide a definition of ″incompatible″ in Article 14(2)(a) prohibiting States receiving evidence from further processing it for ″incompatible″ purposes and to include safeguards to limit the scope of this ″repurposing″;

– the Protocol should include safeguards against the practice of ″forum shopping″ in joint investigations and JITs to prevent Parties from circumventing limitations and prohibitions of certain investigative measures in domestic law;

– public disclosure, by oversight authorities, of data (at least, aggregate information) on the use of the measures under the Protocol and on the number of individuals affected by them should be made mandatory.

17. In a more detailed submission to the Assembly dated 29 July 2021,[8] a group of internet privacy rights advocates forcefully states its opposition to key provisions of the Draft Protocol, in particular direct co-operation with service providers as foreseen in Articles 6 and 7:

> *"Unfettered access to subscriber data can threaten whistleblowers, journalist sources, dissidents, political figures, and others while undermining core privileges and immunities. The Draft Protocol seeks to diminish the sensitive nature of subscriber data and resulting in a range of intrusive powers." (page 1)*

18. The submission points out that according to a survey by the T-CY itself,

> *"many surveyed countries required prior judicial authorisation before law enforcement could access some types of subscriber data. Under Article 7, these States will need to establish a lawful basis for foreign access on a more permissive basis than what is granted to their own law enforcement agencies." (page 4)*
>
> *"Article 7 therefore erodes privacy standards even where appropriate protections already exist. We recommend that Article 7 be removed in its entirety from the text of the Protocol." (page 5)*

19. The submission further notes that:

> *"Imposing time and scope limits on Article 7's reservation mechanism effectively commits States to a particular level of protection despite the ongoing evolution of jurisprudence in relation to subscriber information" (page 7). "It therefore urges the drafters of the Protocol to ensure that parties can remove subscriber information from Article 7 in accordance with jurisprudential and legislative developments over time, by allowing reservations and declarations to be made also after signing and ratifying the Protocol" (page 8).*

20. The authors also recommend introducing mandatory notification or consultation of authorities in the requested Party so that they can apply grounds for refusal, if necessary, and instruct the service provider not to disclose the subscriber information in such cases (Recommendation 5, page 9). They also demand that subscriber data requests must provide enough factual context and explanation of investigative relevance if subscriber data requests are to be properly assessed for their impact on fundamental rights.″

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

(Recommendation 6, page 10). Another key recommendation is that the Protocol must establish independent judicial authorisation as a minimum threshold for cross-border access to subscriber data, or at least allow parties to require such independent judicial authorisation (Recommendation 7, page 11).

21. The submission also strongly criticises Article 12 on joint investigations and joint investigation teams. They should be more limited in scope and duration and be subjected to authorisation by central authorities and prevented from bypassing core safeguards by "forum shopping" (pages 12-17). It also proposes a new Article 13b on confidentiality to ensure that investigative confidentiality conditions are not abused (page 18).

22. The submission welcomes in principle the inclusion of detailed safeguards in the Protocol. But it considers that

> *"The optional nature of Article 14 undermines its utility and stands in stark contrast to the mandatory nature of the Protocol's lawful access obligations. One of the most problematic aspects of the Protocol and its underlying Convention has been that it mandates specific lawful access obligations while requiring human rights and privacy safeguards in only a general sense, to be determined by national law in each of its diverse signatories. […] However, these provisions do not ensure a level of data protection which is consistent with modern data protection instruments such as Convention 108/108+." (pages 19-20)*

23. Last but not least, the Council of Bars and Law Societies of Europe (CCBE)[9] submitted a number of critical comments and made proposals for improvement that it considers as "minimum requirements". A number of them correspond to similar proposals made by the EDPB and the FRA, in particular to establish a general prior judicial review mechanism including a framework for the protection of legal professional privilege and professional secrecy, to require notification of the requested State's authorities before data will be transferred to the requesting State by a service provider to whom a production order was addressed; to clarify and strengthen grounds for refusal to execute international production orders; if requested data are covered by professional secrecy or legal professional privilege, this should constitute an absolute ground for refusal; to ensure that suspected or accused persons or their lawyers are able to request international production or preservation orders in an equally efficient way as is possible for law enforcement authorities (the principle of equality of arms). Finally, and this is a point made only by the CCBE, the Protocol should mention explicitly that lawyers shall have the possibility to participate in a hearing conducted by video conference in order to defend their clients' interests.

5. Assessment of the comments and proposals

24. As a start, it should be recalled that the very purpose of this Protocol is to provide sharper tools to investigate crimes and obtain justice for victims. Given the prevalence of cybercrime today, and the low number of sanctions imposed on perpetrators, it is important to provide victims of online crime a better chance at obtaining justice and to substantially increase the risk of being sanctioned for perpetrators of such crimes. Cybercrime, such as ransomware attacks, has caused considerable economic damage and even loss of life, as certain criminals do not even stop short of attacking hospitals and other critical infrastructures. As recent reports on exchanges between the Presidents of the United States of America and of the Russian Federation[10] have shown, cybercrime is even a threat to world peace. Implicit threats of retaliation for attacks against critical infrastructures by actors that may or may not act on behalf of, or with the tacit toleration by governments might lead to further escalation, with potentially horrific consequences.

25. It should also be recalled that the Second Additional Protocol to the Cybercrime Convention is a criminal justice instrument which applies to specific criminal investigations or proceedings related to cybercrime and evidence on computer systems, as explained in its Article 2 on the scope of application. This means that it is neither an instrument for national security purposes, nor does it provide for mass surveillance or bulk collection of data. It is also not intended to establish or harmonise comprehensive data protection regimes. The Cybercrime Convention has currently 66 Parties, including 21 that are not member States of the Council of Europe and 40 that are not members of the European Union. The Protocol therefore needs to leave a sufficient level of flexibility to permit adaptation to different legal systems and to evolving technology, business models and interpretations by courts.[11]

---

9. CCBE comments on the Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (version 12 April 2021), dated 30 April 2021.

10. See for example https://nypost.com/2021/07/27/in-jab-at-putin-biden-warns-cyberattacks-could-cause-shooting-war. https://www.bbc.co.uk/news/world-us-canada-57786302; How Will Biden Respond to the Latest Cyberattacks? (foreignpolicy.com).

26. This means that an attempt to fully implement the Council of Europe and European Union acquis on privacy rights and data protection in the Cybercrime Convention and its Additional Protocols and to make this mandatory for all Parties, might well fail. This would jeopardise the very purpose of these legal instruments – which is also about protection of fundamental rights – those of the victims of cybercrime – and, as we have seen, about the functioning of the rule of law and democracy. I therefore tend to agree to a large extent with the drafters of the Protocol as it is before us.

27. This said, a number of the proposals submitted by the EDPB, FRA, various civil society groups such as the Electronic Frontier Foundation (EFF) and the Council of Bars and Law Societies of Europe (CCBE) make sense in that they do not seem to endanger the purpose of the Protocol whilst improving the protection of all data subjects in a concrete way. Here is a list of these possible improvements, based on the 15 proposals that I had tentatively assessed as positive in my introductory memorandum. In light of the experts' contributions at our committee hearing on14 September 2021, I have opted to maintain the following proposals:

1. enshrine the application of the principle of proportionality in the text of Article 13, in addition to this being mentioned in the explanatory report[12]

In my view, the principle of proportionality is central to the protection of fundamental rights and belongs in the text of the Protocol itself. This is true even if the principle is mentioned in the Draft Protocol's explanatory report and Article 15 of the Cybercrime Convention, which mentions this principle, is incorporated in the Draft Protocol via its Article 13. Reference in the text of the Protocol itself makes a strong statement in favour of this fundamental human rights principle, which will thus carry extra weight for the interpretation that will be given to the Protocol in practice.

2. specify in Article 14 paragraph 2 that the further processing of personal data by the receiving Party should be provided by law, and should constitute a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest

This proposal is an adequate reflection of the usual formula used by the European Convention on Human Rights, as interpreted by the Court, to assess limitations placed on the right to privacy enshrined in Article 8 of the Convention. Like the first proposal, above, it may be technically ″redundant″, as the T-CY experts explained, but it sends a strong message to the 47 States Party to the European Court of Human Rights, which should influence the future interpretation of this provision in a human rights-friendly sense. In order to accommodate the consideration of the T-CY experts that States that are not party to the European Court of Human Rights may use different concepts or terminology and may be deterred from signing up to the Draft Protocol because of this European Court of Human Rights-based language, the proposal could be supplemented by the words ″*or shall otherwise provide for the adequate protection of human rights and liberties*.″ (as in Article 15 of the Convention incorporated by Article 13 of the Draft Protocol).

3. include in the list of information to be made available to data subjects under Article 14 paragraph 11 the contact details of the competent data controller

This would facilitate the use of the data subjects' information rights in actual practice and should not place a significant burden on the competent authorities.

4. as a general rule, information to individuals related to access and rectification shall be provided free of charge, as an update of Article 14 paragraph 12(b)

In the existing text of the Protocol, it is stated that the ″expense incurred in obtaining access should be limited to what is reasonable and not excessive.″ But the best practice in many countries is that such access should be provided free of charge, except in cases of obvious abuse, such as in the case of repetitive requests on the same grounds.

---

11. See Summary of comments on opinions by Council of Europe Committees and submissions by other stakeholders on the Draft Second Additional Protocol to the Convention on Cybercrime (May 2021), Note prepared by T-CY Secretariat, T-CY (2021)12 dated 28 May 2021 (hereinafter: "Summary paper"), pages 3-4.

12. In the following, the *italicised* text sums up the respective proposals made by stakeholders, followed by brief preliminary assessments in regular script.

5. ensure the respect of safeguards attached to personal data such as privileges and immunities of certain professions

Safeguards for professional privileges and immunities (for example those of lawyers, medical practitioners, religious ministers, or parliamentarians) should indeed be laid down expressly in the Draft Protocol.

6. make public disclosure, by oversight authorities, of data (at least, aggregate information) on the use of the measures under the Protocol and on the number of individuals affected by them mandatory

This proposal deserves our support, as far as it is limited to aggregate information. It would increase transparency and thus promote public trust in the instruments provided by the Protocol, and it would facilitate the evaluation of the functioning of this instrument. The disclosure of aggregate information cannot endanger ongoing investigations or lead to the disclosure of sensitive personal data.

7. in the provisions allowing evidence-taking by video conferencing, to accommodate witness protection measures available at national level; and to include the possibility for lawyers to participate in a hearing conducted by video conference to defend their clients' interests

These proposals by the CCBE make eminent sense, as cybercrime is often committed by organised criminal groups, which are known to threaten and even eliminate witnesses; and the fundamental right to be assisted by a lawyer should also be respected in evidential hearings conducted via video conference.

8. to enhance "equality of arms" between prosecution and defence by foreseeing that at national level, the Contracting Parties' competent authorities may also act on behalf of the defence

Again, this proposal makes good sense. It is obviously in the interest of human rights and the rule of law that accused persons, who are presumed innocent, have the same access to evidence as the prosecution.

28. By contrast, some other proposals by different stakeholders seem to be incompatible with the nature and the purpose of the Protocol, namely, to provide a platform for co-operation in the fight against cybercrime open to as many States as possible, including ones that have not, or not yet, reached the level of data protection achieved by the GDPR or the Council of Europe's European Convention on Human Rights and Convention 108+. Some also seem to be unnecessary, either because the Draft Protocol already covers the issues raised in the proposals, or because any clarifications needed have already been made in the Protocol's explanatory report.

29. This applies to the following proposals:

– *to delete Article 7 on disclosure orders addressed directly to internet service providers*: this would defeat the purpose of the Protocol by taking away an efficient instrument intend to help unclog the existing mutual legal assistance mechanisms passing through over-burdened national central authorities; the limited scope of Article 7 orders and the safeguards in Articles 13 and 14 in conjunction with those existing in the criminal justice systems of the Parties themselves should prevent violations of privacy;

– *to introduce mandatory notification or consultation of authorities in the requested Party by the requesting Party or the requested service provider*: to make such a requirement mandatory would impose a heavy administrative burden on those Parties which do not consider it necessary to be notified systematically of requests addressed to service providers. This would undermine the purpose of the Protocol to unclog the existing mechanisms;

– *subscriber data requests must provide enough factual context and explanation of investigative relevance as subscriber data requests are to be properly assessed for their impact on fundamental rights*: this is not needed, as Article 7.4. already foresees that information shall be provided on the domestic legal grounds that empower the authority to issue the order and a reference to legal provisions and applicable penalties for the offence being investigated or prosecuted. To require additional information on the facts of the investigation or proceeding and the relevance of the subscriber information to the investigation or proceeding would impose an undue burden both on the requesting authority and the requested service provider, given the limited scope of requests under Article 7.

– *to clarify the binding nature of the data protection safeguards in the Draft Protocol*: any binding rules beyond those already included in Articles 13 and 14 of the Draft Protocol would risk making this instrument inaccessible to States outside the European Union or the Council of Europe. The safeguards already agreed by the drafters constitute real progress requiring considerable efforts from a number of countries that still have a weaker data protection regime;

– *to ensure the systematic involvement of a judicial or an independent administrative authority in the requested Parties, except in cases of validly established urgency*: such a requirement would, again, risk defeating the very purpose of the Protocol. Article 14 paragraphs 13 and 14 of the current draft Protocol provide for ″effective judicial and non-judicial remedies to provide redress for violations″ [and that] Each Party shall have in place one or more public authorities that exercise, alone or cumulatively, independent and effective oversight functions […] The functions […] shall include investigative powers, the power to act upon complaints and the ability to take corrective action.″ To add systematic preventive review to these remedies would risk defeating the purpose of the instrument, namely, to provide for rapid, unbureaucratic international co-operation in the fight against cybercrime. In my view, it would be disproportionate to require judicial authorisation with regard to requests for domain name registration information, given that requests are limited to specific criminal investigations and proceedings; disclosure is subject to reasonable conditions provided by domestic law; and the safeguards of Articles 13 and 14 apply;[13]

– *to develop further specifications and requirements regarding security and authentication of the bodies empowered to request and receive data*: it would be impossible to prescribe a single system, beyond Article 6, whose purpose it is to provide a legal basis for a system of access to domain name registration information that is being developed in the Internet Corporation for Assigned Names and Numbers (ICANN) context. Service providers and criminal justice authorities have widely different security and authentication requirements. The Draft Protocol (Articles 6 and 7) therefore limits itself to stating that the relevant authorities shall require appropriate levels of security and authentication, but leaves the details to the Parties;

– *to clarify the definition of subscriber information in order to avoid inclusion of any traffic or content data*: this is not necessary, as the term ″subscriber information″ is well-defined in the Cybercrime Convention itself (Article 18 paragraph 3.), which the Draft Additional Protocol merely supplements. Moreover, paragraphs 92 and 93 of the explanatory report already provide the clarification that traffic data are excluded from the definition of ″subscriber information″;

– *to tighten the rules governing the establishment and operation of joint investigation teams under Article 12, in particular to include safeguards against the practice of "forum shopping" in joint investigations and joint investigation teams to prevent Parties from circumventing limitations and prohibitions of certain investigative measures in domestic law and to require the central authorities' approval of JIT agreements*: this is not necessary, as the participating Parties can only do what is permitted under their domestic law. When measures are carried out in a Party participating in a JIT, the authorities of that Party determine whether they can take the investigative measure on the basis of their domestic law; and JITs are subject to all the oversight mechanisms of the criminal justice systems concerned;[14] JITs have proved to be efficient tools for international co-operation against organised crime and their establishment and operation should not be stifled.

– *to insert a new paragraph 13b to ensure that investigative confidentiality conditions are not abused:* this is not necessary, as Article 14 paragraph 12 of the Draft Protocol provides a general right of access and rectification for individuals whose personal data have been received. Sub-paragraph a. *i*. already foresees that:

> *"access in a particular case may be subject to the application of proportionate restrictions permitted under its domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned."*

– *to provide a definition of "incompatible" in Article 14 paragraph 2 (a) prohibiting States receiving evidence from further processing it for "incompatible" purposes and to include safeguards to limit the scope of this "repurposing"*: this is not necessary, as the term ″incompatible purpose″ is explained clearly in paragraphs 227 pp. of the explanatory report. ″Compatible″ are the purposes described in

13. See "Summary paper" (note 9), Section 4.1.3.
14. See "Summary paper" (note 9), Section 4.1.10.

Article 2, that is for the purpose of ″specific investigations or proceedings concerning criminal offences related to computer systems and data″ and for the ″collection of evidence in electronic form of a criminal offence″.

– *to clarify in Article 14 that the Draft Protocol applies to Parties, unless another agreement or arrangement between the concerned Parties provides the same or higher level of protection regarding privacy and the protection of personal data than the Protocol itself*: again, such an amendment would risk excluding co-operation between Parties whose data protection regime has not yet reached the level of the GDPR or Article 8 of the European Convention on Human Rights;

– *to amend Article 14 paragraph 6, concerning automated decisions, to clarify, in addition to human intervention, that safeguards under domestic law of the Parties authorising such processing provide guarantees for the rights and freedoms of the data subject*: this amendment seems unnecessary. Once human intervention takes place, which is foreseen in the existing text as one of the ″appropriate safeguards″ required, the general safeguards in place under Articles 13 and 14 of the Draft Protocol apply;

– *to complement the provisions under Article 14 paragraph 12 in order to ensure that any individual may seek and obtain information as to whether or not personal data concerning him or her are being processed*: this seems to be already the case, as under Article 14 paragraph 12 a. i. the data subject is entitled to receive a copy of the documentation kept on that individual, complete with information on the legal basis for and purposes of the processing, retention periods and recipients of the data, as well as available options for redress;

– *to clarify Article 14 paragraph 13 on effective remedies so as to ensure that both judicial and non-judicial remedies are available under the jurisdiction of each Party to the Cybercrime Convention to any concerned data subjects*: again, this seems to be already clear in the existing draft. Paragraph 13 reads: ″Each Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of this article.″

– *to require Parties to the Additional Protocol to accede to Convention 108+:* whilst it is highly desirable that as many Parties to the Cybercrime Convention and its Additional Protocols are also Parties to the Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) and its additional Protocols, making this a requirement would exclude a number of potential Parties from signing up to the Draft Protocol whose co-operation in the fight against cybercrime is equally desirable, in accordance with the Protocol's purpose. This said, I suggest that in its Opinion, the Assembly shall call on all States wishing to sign up to this Protocol to also consider sign and ratify Convention 108+.

– *to stress the "ne bis in idem principle" in order to avoid double penalization of a witness in case of perjury or similar offences, when both States administered the oaths or other warnings*: the principle of *ne bis in idem* is generally recognised in national criminal law and does not need to be laid down specifically in this Protocol for one very specific situation.

30. In light of the experts' presentation during our hearing on 14 September 2021[15], I also refrain from taking on board the following proposals, which I had given a preliminary positive assessment in my introductory memorandum, namely:

1. to clarify in Article 14 paragraph 1(a) that personal data received by requested authorities or private entities as included in the request shall be protected in the same way as the personal data received by the requesting authorities:

I considered initially that such a clarification would close a potential ″loophole″, as the requests themselves often contain personal data that require protection in the same way as the data received in response to such a request. But as the T-CY experts pointed out, Article 14 paragraph 1. in conjunction with paragraph 221 of the explanatory report already ensures that Article 14 applies to all personal data a Party receives under this Protocol applies, including such data as are part of the request.

15. See appendix.

2. to allow the Party transferring personal data (within a request or in a reply to a request) to require from the receiving Party additional safeguards or to allow the requested Party to refuse such transfer so as to ensure that the level of protection of personal data under European Union law is not undermined:

I considered initially that such a safeguard clause may well be necessary in order to avoid undermining the European Union acquis on data protection, which could make participation of European Union member States in the co-operation mechanisms established by the Protocol legally problematic. But the T-CY experts convinced me that the Draft Protocol fulfils the core requirements of EU law (in particular, Article 46 GDPR and Article 37 of the Data Protection Law Enforcement Directive). Trying to impose on non-EU member States a full ″photocopy″ of EU data protection rules may well make ratification by many of them very problematic. But in order to respond to legitimate criticism, it would be useful if the explanatory report on Article 14 were revised to better explain the interrelation between the different data protection regimes foreseen in this Article.

3. to replace, in Article 14 paragraph 4, the words "considered sensitive in view of the risks involved" by "which allow or confirm the unique identification of that natural person":

I considered initially that the new formulation proposed is less subjective (″considered sensitive″ – by whom?) by focusing on the main risk involved, namely that of allowing or confirming the identification of a natural person; but the T-CY experts convinced me that the existing formulation, by focusing on the risks involved, provides the needed flexibility to accommodate the evolving field of biometric data. Moreover, in their opinion, the proposals for amendments actually narrow down significantly the application of the safeguards. This runs contrary to the scope of protection offered by Article 14 of the Draft Protocol.

4. to include in paragraph 6 a specific provision prohibiting the processing of sensitive data for the purpose of automated decision-making, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are explicitly mandated for under paragraph 6:

I initially considered that this proposal rightly takes into account the specific risks involved in automated decision-making, when sensitive data are involved, which require suitable safeguards. But the T-CY experts pointed out that paragraph 6, as drafted, already provides for such safeguards, and it is aligned with existing standards, including Convention 108+.

5. to remove the time and scope limits on Article 7's reservation mechanism:

I initially considered that it would indeed make sense to allow some flexibility for Parties to react to jurisprudential and legislative developments over time, and not only at the time of the signature and ratification of the Protocol. But I am now convinced that allowing for reservations and declarations after the signature and ratification would be too far removed from established State practice concerning the signature and ratification of treaties.

6. to explicitly extend the application of Article 14 paragraph 8 (on maintaining records) to any processing activities and in particular to "storage":

It is indeed important, for the reasons of transparency and public trust in the mechanism established by the Protocol that records are kept on any processing activities, which must include storage of data, which in turn can be a particularly risky activity. But the T-CY experts recalled that Article 25 of the EU Law Enforcement Directive and Convention 108+ also do not provide for such a requirement and convinced me that requiring detailed record keeping of each storage activity would constitute an excessive burden that a number of Parties would not be willing to bear.

7. to clarify and specify the conditions under which information rights of data subject rights may be restricted in order to be fully consistent with EU law and the European Convention on Human Rights, and notably meet the foreseeability and proportionality criteria:

I initially understood that the Draft Protocol as it stands does not lay down the permissible grounds for the denial or restriction of access rights clearly enough and that these should therefore be clarified, as proposed by the EDPB. But the T-CY experts recalled the list of four limits for restrictions placed upon the data subject's rights in Article 12: *firstly,* that the restrictions must be proportionate and permitted under the domestic legal framework; *secondly,* that they are still ″needed″ at the time of adjudication; *thirdly*, that they serve to protect the rights and freedoms of others or other important objectives of general public interest; *fourthly,* that they give due regard to the legitimate interests of the individual concerned. This test also seems to be in line with EU data protection law (for example Article 23(1) GDPR) and Convention 108+.

8. to further clarify the reasons for which a service provider may lawfully refuse to disclose subscriber information; violations of fundamental rights in the requesting or requested State should be recognised as such a reason, as should be the fact that the information requested is covered by legal privilege:

I initially supported these proposals by the FRA and the CCBE as they would further enhance the credibility of the Draft Protocol from a human rights perspective. Such a clarification would make it less risky for service providers to refuse transmitting user data in doubtful cases. But the T-CY experts explained that the Draft as it stands leaves several options to Parties, including that to grant unfettered discretion to providers to refuse orders, or to require notification of orders served on providers in its territory and to instruct the provider not to comply with the order based on grounds for refusal foreseen in Article 25 paragraph 4 and Article 27 paragraph 4 of the Cybercrime Convention, including refusal for ″essential interest″ reasons (namely human rights concerns). Finally, an exhaustive list of grounds would not be feasible, whilst a general clause would put providers in the difficult position of having to make such a legal determination themselves.

6. Conclusions

31. We have seen that the Draft Second Additional Protocol to the Cybercrime Convention is not a purely technical exercise. It raises considerable rule of law and human rights issues, in particular the provisions which introduce the possibility of ″direct co-operation″ with providers and entities in other Parties. But it should be recalled that the Protocol will function within the criminal justice systems of the Parties with all the procedures, regulations, methods for transmitting data, conditions, and safeguards. This applies also to the ″direct co-operation″ provided by Articles 6 and 7, both of which require Parties to establish a proper domestic legal basis for the exercise of these powers.

32. The purpose of the Draft Protocol – to facilitate international co-operation in the fight against cybercrime – is itself directly related to upholding the rule of law and protecting the fundamental rights of the victims of cybercrime.

33. The comments and proposals made by different stakeholders deserve to be taken seriously. However, if the Draft Protocol is to fulfil its purpose, they cannot all be taken on board by the drafters. In chapter 5 above, I have explained my position on a number of key proposals. Whilst I support some of them, I am more sceptical with regard to others. My conclusions on these proposals, which I have finalised in light of the experts' presentations during our committee meeting on 14 September 2021, are reflected in the draft Opinion preceding this explanatory report.

Appendix - Hearing on 14 September 2021

At its meeting on 14 September 2021, the committee heard presentations by three experts:

– the Chairperson of the Cybercrime Convention Committee (T-CY) in charge of drafting the Protocol, Ms. Cristina Schulmann (Romania),

– its Executive Secretary, Alexander Seger,

– Ms Katitza Rodriguez (Electronic Frontier Foundation/EFF).

Ms Schulman and Mr Seger both argued in favour of keeping the current draft texts unchanged, whereas Ms Rodriguez proposed a number of amendments and reiterated the criticism expressed by civil society on certain provisions of the Draft Protocol.

Ms Schulman, presented the context of the Draft Protocol and argued in favour the need for its speedy adoption. She explained the complex and inclusive negotiation process involving States from all regions of the world with different legal systems, including the 21 States that are not members of the Council of Europe. The Protocol should work for all of them. She noted that the Draft Protocol was drafted to provide governments with the means to fulfil their positive obligations to protect persons against violations of their rights caused by cybercrime. She added that according to the drafters of the Protocol this could be done by providing additional tools for effective investigations and prosecutions through enhanced co-operation between the Parties to the Cybercrime Convention. She pointed out that cybercrime had known no borders and that it had reached an unprecedented level of proliferation. The Second Additional Protocol would help to resolve a number of challenges for the investigation of these crimes, such as difficulties in obtaining electronic evidence, usually located in foreign, multiple or even unknown jurisdictions and possessed by private entities. Thus, the main functions of the Draft Protocol, as she emphasised, were to enable direct co-operation with service providers and other entities for the disclosure of subscriber information and domain name registration data; to simplify the procedure for the production of subscriber information and traffic data from other Parties; to improve international co-operation in emergency situations, including by establishing JITs and establishing rules for video conferencing where other treaties did not regulate them. Ms Schulman, underlined that these measures should be subjected to a particularly strong system of safeguards, including Article 14 on the protection of personal data as a unique provision for a criminal justice treaty. The conditions and safeguards of Article 15 of the Cybercrime Convention, including the principle of proportionality, were incorporated into the Draft Protocol via its own Article 13. She emphasised, moreover, that the scope of the Draft Protocol was narrow, namely it pertained to specific criminal investigations and the gathering of electronic evidence during the proceedings related to cybercrime. The Draft Protocol was not meant to be a treaty on harmonising data protection legal regimes or to regulate cybersecurity systems or to allow mass surveillance. The Protocol represented a carefully calibrated text designed to be consistent with the acquis of the Council of Europe but also to meet the requirements of all other Parties to the Cybercrime Convention. Ms Schulman, stressed that to reopen any paragraph of these draft texts may affect this careful compromise.

Mr Seger reiterated that many stakeholders, including those mentioned in the Rapporteur's introductory memorandum, were invited to and heard during the negotiations and drafting process. Comments received from civil society and other stakeholders were either reflected in the Draft Protocol or were considered as redundant and unfeasible. Addressing the proposals mentioned in paragraph 21 of the Rapporteur's introductory memorandum, he underlined that all of them were taken into consideration. Some of them provided no added value in relation to the current, carefully drafted text. For example, the proposal to include a specific reference to the principle of proportionality in Article 13 was not needed since all conditions provided by Article 15 of the Cybercrime Convention – including but not only the principle of proportionality – were incorporated into the Draft Protocol. The second proposal was also irrelevant because draft Article 14 paragraph 1 (a) could be applicable to any ″personal data received under [the] Protocol″ and therefore the requests to other public authorities could not contain the alleged ″loophole″ regarding personal data. The next proposal, in relation to the definition and sensitivity of biometric data under Article 14 paragraph 4 of the Draft Protocol, was dismissed by the drafters for the considerations that the Parties had different understandings of the meaning ″sensitive″ as continuously evolving concept. The current draft text, therefore, represented a compromise allowing for some flexibility in its interpretation and application in practice. Due to the time constraints, Mr Seger then referred the committee and the Rapporteur to the written comments on the remaining proposals.

Ms Rodriguez strongly disagreed with both previous speakers. She considered that the Draft Protocol failed to impose ″clear and enforceable baseline safeguards in cross-border evidence gathering″ and, most importantly, regretted that the privacy protections provided in the Draft Protocol were mostly ″optional″ rather than mandatory. The police powers regulated by the Draft Protocol were excessively intrusive, especially as

regards ″direct co-operation″ between the investigative authorities of one State Party with private entities holding sensible private data (Articles 7 and 12) in another. She suggested to remove these provisions entirely or at least to improve them by providing strong procedural safeguards for the requests for data as foreseen by Convention 108+. This Convention should remain the authoritative legal instrument in this area, even for the Draft Protocol. She suggested that accession to the Protocol should be made conditional upon signing up to Convention 108+. She was particularly concerned about the possibility offered by the Draft Protocol for governments to enter into secret bi- or multilateral agreements and setting up arrangements that would be less protective than the established international standards, whilst using the powerful tools provided by the Protocol. She also criticized the Protocol's regulations on JITs and addressed a question in this respect to Mr Seger. He replied that a careful reading of the text of Article 12 on JITs would show that the concerns raised by Ms Rodriguez – regarding the duration of a JIT agreement and the applicable law of the Party where investigative measures are undertaken – were all thoroughly addressed by the drafters of the Protocol. Moreover, he underlined that this article regulating the activity of JITs, like all other measures provided by the Draft Protocol, were subject to the safeguards of Articles 13 and 14.