PACE/Committee on Legal Affairs and Human Rights:
Hearing on the draft Second Additional Protocol to the Convention on Cybercrime
14 September 2021

Draft Second Additional to the Budapest Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence

Presentation by

Cristina Schulman, Chair of the Cybercrime Convention Committee (T-CY), Ministry of Justice of Romania

and

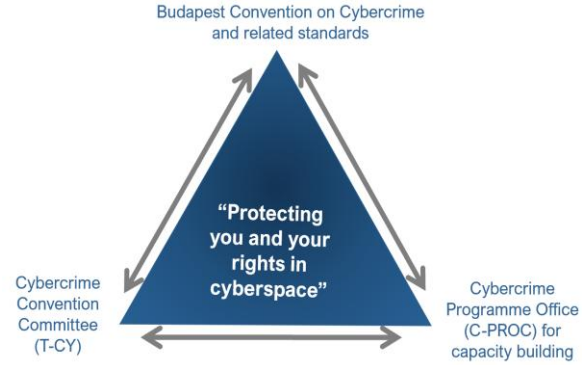
Alexander Seger, Executive Secretary of the T-CY, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Context

- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 11 signatories and States invited to accede
- ✓ 120+ States with substantive laws aligned with BC
- ✓ 150+ States have used it as a guideline or source
- ✓ 180+ States have been participating in COE activities on cybercrime
- ✓ Promoting rule of law and human rights in cyberspace

► **Multilateral instrument – the same expected from 2nd Protocol**



Challenges

Cybercrime: Threat to

- Human rights
- Democracy
- Rule of law

Positive obligations:

- Provide the means to protect the rights of individuals, also against crime

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- Effective means not available to obtain the disclosure of e-evidence
- Less than 0.1% of offences in cyberspace lead to prosecutions and convictions
- Do victims obtain justice?

→ 2nd Protocol to help address these challenges

Draft 2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence: content

Means for a more effective criminal justice response:

- Direct cooperation with service providers in other jurisdictions to obtain subscriber information
- Direct requests to registrars to obtain domain name registration information
- More effective means to obtain subscriber information and traffic data through government-to-government cooperation
- Expeditious cooperation in emergency situations
- Joint investigations and video-conferencing

Subject to a particularly strong system of safeguards:

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
- Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty
- Articles specify types of data to be disclosed
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided

Draft 2nd Additional Protocol to the Convention on Cybercrime: the process of negotiations

Protocol:

- Prepared by Protocol Drafting Plenary and Drafting Groups established by the Cybercrime Convention Committee September 2017 to May 2021
- 91 sessions of the PDP, PDG and PDG subgroups
- 75 States and several international organisations participated with over 620 experts
- Data protection experts participated in negotiations
- 6 rounds of stakeholder consultations

= 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 Budapest Convention

5

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

1. Enshrine the application of the principle of proportionality in the text of Article 13, in addition to this being mentioned in the explanatory memorandum

Comment

A specific reference to proportionality in the text is not needed for two reasons:

- Incorporating Article 15 of the Convention into this Protocol via Article 13 means that the principle of proportionality as well as the other conditions and safeguards of Article 15 are applicable to the Protocol. Referencing only proportionality would create doubts regarding the other principles.
- Parties apply the principle of proportionality in accordance with relevant principles of domestic law as agreed in the Convention (see ER para 146 to the Convention). If proportionality specifically mentioned in text, related principles of other Parties would also need to be spelled out.

6

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

2. 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

Comment

- Article 14.1.a states that Article 14 applies to "personal data that it receives under this Protocol" including as part of a request (see paragraph 221 ER). There is thus no loophole when it comes to public authorities.
- The Protocol cannot bind private sector entities. Domestic data protection rules are expected to apply to such entities. A Party may also issue procedural instructions to a provider for confidentiality (see paragraph 106 of the ER).

7

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

3. 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.

Comment

- EU COM participated in negotiations to ensure that requirements of EU law are met. Under EU data protection law an international agreement ensuring 'appropriate safeguards' may be a ground for transfers (Article 46 GDPR and Article 37 Law Enforcement Directive). No need for exact copy of EU law but to ensure the core data protection principles, rights and obligations are available under EU law. The Protocol fulfils this requirement.
- Article 14 of the Protocol was included to create certainty for all Parties: if the data protection conditions of this Article are met, Parties should be able to receive personal data from other Parties free from other general data protection conditions (see Article 14.1.d). This does not preclude that a Party may impose other conditions in specific cases pursuant to the Protocol according to Article 14.2.a.
- If some Parties could at any time impose additional data protection requirements, the benefits of Article 14 would be limited.
- See also Article 14.14 on assessments and Article 14.15 on consultations/suspension.

8

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

4. 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.

Comment

- Article 14.2.a already provides that a Party "shall not further process the personal data for an incompatible purpose, and it shall not further process the data when this is not permitted under its domestic legal framework".
- The terms "domestic legal framework" is used in Article 14.2 to accommodate different legal systems.
- Parties that are not M/S of the CoE may apply related principles of their domestic law.
- Article 15 Convention incorporated via Article 13 already requires conditions and safeguards that "shall provide for the adequate protection of human rights and liberties".

9

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

5. 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".

Comment

The terms "considered sensitive in view of the risks involved" was a necessary compromise after lengthy discussions during negotiations for the following reasons:

- Parties may have a different understandings of the term "biometric data".
- Biometric data is an evolving field and what is considered sensitive may also evolve over time.
- Not all biometric data is equally sensitive. For example, an image in a newspaper, footage in a video or TV broadcast, tattoos or scars may not fall into the same category of sensitive biometric data.
- Some flexibility is therefore needed for Parties to interpret what type of biometric data require stronger protections considering the risks involved.

10

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

6. 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

Comment

- Appropriate safeguards for sensitive data are covered by paragraph 4 and safeguards for automated decision-making by paragraph 6, and furthermore personal data are processed for the purposes of criminal investigations or proceedings (see Article 14.2. a with reference to Article 2 of the draft Protocol).
- Parties considered therefore that this combination provides the necessary safeguards.
- Paragraph 6 is already broadly aligned with existing standards, including Convention 108+.

11

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

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

Comment

- Article 14.8 focuses on the larger principle that Parties need to have effective means for demonstrating how the data of a specific individual have been accessed, used and disclosed so as to permit oversight and accountability. The precise means is left to the discretion of Parties.
- It is unclear what a record would need to show in terms of "storage" and what the added value would be.
- Requiring detailed record keeping of each processing and storage activity would be an excessive burden and during the negotiations was not considered to be workable by a number of Parties.

12

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

8. 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.

Comment

- Either through general notices, or through personal notice, the data subject will already be able to obtain / have obtained details of the competent data controller that has received his/her personal data under the Protocol.
- Through access requests an individual may obtain additional information.
- Oversight authorities (Article 14.14) also have the power to act upon complaints and the ability to take corrective action.

13

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

9. 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 the European Convention on Human Rights, and notably meet the foreseeability and proportionality criteria

Comment

- The requirement to provide access and rectification free of charge may conflict with existing laws and regulations of a number of Parties that permit reasonable and not excessive cost, inter alia, to prevent abusive requests or requests requiring an extraordinary amount of resources to respond to. This is therefore best left to the domestic law of Parties. Paragraph 12.b represents a compromise that the cost be limited “to what is reasonable and not excessive”.
- Convention 108+ also allows Parties to charge a “reasonable fee” for access.

14

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

9. 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 the European Convention on Human Rights, and notably meet the foreseeability and proportionality criteria

Comment

Paragraph 12 limits restrictions to those:

- that are proportionate and permitted under the domestic legal framework;
- that are needed at the time of adjudication;
- that have been put in place to protect the rights and freedoms of others or other important objectives of general public interest;
- that "give due regard to the legitimate interests of the individual concerned".

This rather long, detailed and well-balanced list is the result of complex negotiations and found to meet the requirements of different Parties.

15

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

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

Comment

- The Protocol cannot cover how immunities or professional privileges are applied at domestic levels. Parties would apply their existing processes and procedures. (This is not harmonized COE- or EU-wide.)
- The Protocol contains some safeguards. For instance, paragraph 141 of the ER explains that Article 8.8 provides grounds for refusing a request with reference to "safeguards for the rights of persons located in the requested party".
- Regarding the direct cooperation Articles 6 and 7 of the Protocol, these are about the disclosure of WHOIS and subscriber information and are unlikely to include privileged information.
- Privileges and immunities are not data protection safeguards.

16

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

11. Ensure 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.

Comment

- This is not a requirement in other COE treaties.
- Parties may compile and publish such data if required by domestic rules.
- Service providers may continue to publish transparency reports.

17

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

12. 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-link to defend their clients' interests.

Comment

- Article 11.1 already foresees particular modalities that could include witness protection measures and for lawyers to participate ("the authorities and persons that shall be present; .... the manner of questioning the witness; …. the manner in which the rights of the witness or expert shall be duly ensured; the treatment of privileges and immunities …").
- In addition, this Article gives the requested Party discretion whether or not to accept the request or to set conditions for providing assistance (ER para 188).
- The Protocol is not an instrument meant to harmonise the requirements for video-conferencing in the Parties, but it allows reconciling the requirements of the domestic laws of both the requesting and requested Party, including with regard to procedural rights, and thereby facilitates the cooperation.

18

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

13. 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.

Comment

- Establishing a general rule on this would be outside the scope of this Protocol and has also not been addressed in the Convention on Cybercrime or in other treaties.
- Whether a court in a Party issues an order on behalf of the defense and in what circumstances is a matter for that Party's domestic law, as is the manner in which the other Party responds.
- In some Parties such requirement may also lead to conflicts of interest situations.
- Considering the different approaches Parties take in relation to this matter, specifying these elements in the Protocol could also interfere with Parties' domestic legal approaches and undermine their ability to accede to the Protocol.

19

Draft 2nd Additional Protocol: Comments on some suggestions by stakeholders

14. 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.

Comment

- No need to clarify the reasons that providers may refuse to disclose the requested information, as the Article itself already provides for sufficient safeguards in this regard.
- For example, under Article 7.5.c, a Party requiring notification could choose to instruct the provider not to comply with the order based on grounds of refusal established in Article 25, paragraph 4, or Article 27 paragraph 4 of the Convention.
- No need to establish additional grounds for refusal that go beyond grounds for refusal used in the context of mutual assistance.
- Application of any particular privilege would be determined and applied by the Party receiving the data. (See comment on proposal 10 above.)

20