02-05-2021

To: the Cybercrime Convention Committee

CC:
Ms Dunja Mijatović
Mr Patrick Penninckx
Mr Alexander Seger
Mrs Alessandra Pierucci
Mr Rik Daems

Subject: 6th round of consultation on the Cybercrime Protocol and civil society participation

Dear members of the Cybercrime Convention Committee,

We, the undersigned organisations and academic, have closely followed the Council of Europe discussions around cross-border access to electronic evidence and the drafting process of the Second Additional Protocol to the Cybercrime Convention, submitting comments during all previous rounds of consultations. The issue is of importance for us for a wide variety of reasons – from defence of the rule of law and the protection of human rights.

Despite our active participation in past rounds of this process, we are concerned that the Committee is rushing through the last stages of negotiations in order to hastily finalise the text of the Second Additional Protocol without meaningful consultation. We note in particular that drafting meetings of the Protocol have been held in closed sessions without the involvement of civil society and other observers, and that this is the first opportunity the public has had to comment on a complete draft of the Protocol. In particular, this consultation is problematic

because the much needed recent provisions introducing human rights safeguards should deserve thorough examination and open discussions. The implications of these provisions are far-reaching and engage several complex principles of law and policy. Unfortunately, the time frame given to provide feedback is largely insufficient. It is therefore **impossible for civil society organisations to submit substantive advice and comments.** We believe this goes **against the Council of Europe's usual standards of accountability, participation, and inclusion. We call for a genuine opportunity to be given to external stakeholders to provide feedback, considering the data protection and other human rights considerations at stake.**

Nonetheless, we would like to share our serious concern that many of our previous recommendations were not taken into account and the most dangerous measures for human rights remain part of the draft. In particular, we believe the following issues deserve further discussion and revision from a fundamental rights perspective:

Intrusive measures creating the potential for serious interference with human rights

- Section 2 still contains measures permitting "direct cooperation" with private entities, thereby encouraging the voluntary disclosure of personal data (domain name registration information, subscriber information) outside of a proper legal framework involving independent judicial authorities in Parties on both sides. **This has severe implications for the rule of law.** Furthermore, there is no mandatory requirement for authentication of (digital) law enforcement requests, notably via the designation of one single competent authority by Party whose information is made available in a public register. **This is critical to mitigate the risk inherent in any cross-border direct disclosure framework that cybercriminals commit identity theft (by impersonating competent authorities) or other cybercrime.**

- We welcome that Article 7(2)(b) allows Parties to require judicial supervision of production orders to service providers on their territory. In light of the critical role of judicial oversight for protection of fundamental rights, **we recommend that judicial authorisation should be mandatory for all production orders under the Protocol. This should also apply to production orders under Article 6**, where the present draft does not allow Parties to require judicial supervision.

- **The scope of the definition of "subscriber data" is overbroad and fails to exclude data categories that would reveal precise conclusions concerning the private lives and daily habits of a subscriber.** The lack of precision with regard to the precise scope of the term leaves it open to broad interpretation and in case this is not clarified, in violation of the principle of legality as established in the jurisprudence of the European Court of Human Rights. Overall, Section 2 fails to acknowledge the threat to anonymity, privacy and human rights posed by the identification capabilities it encodes.

Inadequate human rights protections and independent oversight

- As regards Chapter III on Conditions and Safeguards**, we reiterate our recommendation that Parties to the Additional Protocol should be required to accede to Convention 108+.**

Instead, Article 14 provides a more limited set of data protection obligations for law enforcement authorities of Parties. Even though data protection is a critical element of the Protocol, the draft for Article 14 was not published until 12 April 2021, giving stakeholders insufficient time to respond. Furthermore, the Explanatory Report for Article 14 is still not available. This undermines the principle of transparency and fairness of the drafting procedure.

- In its opinion[1] of 2 February 2021, the European Data Protection Board stressed that "since the Budapest Convention, as well as any of its additional protocols, are binding international instruments, [...] in line with the Court of Justice of the European Union case law, the "obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness". It is therefore essential that **the provisions laid down in the additional protocol do comply with the EU acquis in the field of data protection in order to ensure its compatibility with EU primary and secondary law.**"

- For direct disclosure from private entities in the European Union, Article 14(1)(d) will take precedence over Chapter V of the GDPR which requires an adequacy decision of the third country by the European Commission or an assessment by the data controller that the transfer is subject to appropriate safeguards. **We are concerned that the data protection obligations of Article 14 may not be sufficient to provide appropriate safeguards in line with the requirements of the jurisprudence of the Court of Justice of the European Union (CJEU).** In particular, data transfers can only be suspended if there substantial evidence that the other Party is in systematic and material breach of the terms of Article 14. In C-311/18 the CJEU reiterated the role and the specific powers of supervisory authorities in the context of international data transfers defined in Article 58(2)(j) GDPR, including suspension of transfers. **It is therefore vital that supervisory authorities are involved in the drafting process of the Protocol.**

- Article 14(2)(a) allows States receiving evidence to further process it for "compatible" purposes. **No definition of "compatible" is provided and no safeguards are foreseen to limit the scope of this repurposing.** This is the case for both data obtained through orders under Chapter II and in the framework of joint investigations (Article 12).

- **There is a crucial lack of safeguards against the practice of "forum shopping" in joint investigations and joint investigation teams** which enable Parties to circumvent limitations and prohibitions of certain investigative measures in domestic law (of the territory where the investigation is carried out).

- **There is a lack of mandatory public disclosure of data (at a mininmum aggregate information) on the use of the measures under the Second Additional Protocol and on the number of individuals affected by them** by oversight public authorities established in

1 European Data Protection Board, Statement on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), 2 February 2021, available at: https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf

Article 14(14). Failing to publish such data would result in lack of accountability to the public from competent authorities.

Lastly, we would like to recall that new solutions for mutual legal assistance are possible, but these new solutions need to respect human rights principles. Pre-existing mutual legal assistance frameworks can and need to be reformed appropriately. We call for predictable, accountable legal structures for access to personal data across borders that don't undermine existing data protection standards instead of the currently foreseen far-reaching measures.

Sincerely,

Access Now – International
ARTICLE 19 - International
Dataskydd.net – Sweden
Derechos Digitales – Latin America
Digitale Gesellschaft – Germany
Digital Rights Ireland – Ireland
Electronic Frontier Foundation (EFF) – International
European Digital Rights (EDRi) – International
Fundacion Karisma – Latin America
Homo Digitalis - Greece
IPANDETEC – Central America
IT-Pol – Denmark
Douwe Korff, Emeritus Professor of International Law, London Metropolitan University
Vrijschrift.org – The Netherlands

Annex - Our previous submissions

- Letter to the Council of Europe Steering Committee on Media and Information Society on the final report of the T-CY Cloud Evidence Group (10.11.2016)
- Position paper on the Cybercrime Convention – cross-border access to electronic evidence (17.01.2017)
- Joint Civil society letter to the Secretary General of the Council of Europe on the draft Second Additional Protocol to the Convention on Cybercrime (03.04.2018)
- Joint Civil Society Response to the 2nd Additional Protocol to the Budapest Convention on Cybercrime (28.06.2018)
- Comments on the provisional draft text on "emergency mutual assistance" and "languages of requests" of the Cybercrime Convention Committee (T-CY) (20.02.2019)
- Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime (08.11.2019)
- Joint Civil Society Response to the provisional draft text on "Joint investigation teams and joint investigations", "Expedited disclosure of stored computer data in an emergency" and "Requests for domain name registration information" (15.12.2020)