Eticas Foundation's Oral Intervention on Chapter III, Procedural provisions and law enforcement (agenda item 6)

Delivered By Tanja Fachathaler on behalf of Eticas Foundation Fourth Session - 9 January to 20 January 2023

As held

Representing Eticas Foundation, we appreciate the effort of the Ad-Hoc-Committee, its members and staff for the drafting of the CND, for facilitating the present session and for ensuring that the elaboration of a Cybercrime Convention is an all-inclusive process which includes civil society.

In drafting the procedural provisions and provisions on law enforcement we would like to recommend the following:

- Article 41: [Scope of procedural measures]
The scope of procedural measures should be **limited to the investigation of criminal offences set out in this Convention**. It otherwise risks to **significantly undermine core human rights** – like the right to privacy or the right to a fair trial – if the scope covered all crimes committed with the use of an ICT.

- Article 42: [Conditions and safeguards]
A significant expansion of the provision is required to cover the **following safeguards**:

- A **right to an effective remedy** for violation of privacy must be known and accessible to anyone with an arguable claim that their rights have been violated. As stated by the UN High Commissioner for Human Rights in his report "The right to privacy in the digital age", this requires notice (that either a general surveillance regime or a specific surveillance measures are in place) and legal standing to challenge such measures.
- Effective remedies must also include **prompt, thorough and impartial investigation of alleged violations.** The investigating body needs to have the power to order the end of all ongoing violations as well as full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations and the capacity to issue binding orders.
- A requirement should be added that any investigative powers listed in this Convention must be conducted in ways **not to compromise the security of digital communications and services.** It needs to ensure that the Convention does **not in any way justify government hacking.**

  Government hacking should be outside the scope of this treaty because it is unlike any other form of existing surveillance techniques: It can be far more intrusive than any other surveillance technique, permitting remote and secret access to personal devices and data stored on them, as well as to conduct novel forms of real-time surveillance (like turning cameras or microphones on), manipulate data on devices while erasing any trace of the intrusion. It also affects the privacy and security of others in unpredictable ways. And it exploits vulnerabilities in systems to facilitate surveillance objectives.

  In short: government hacking is at cross with digital security aims.

Madam Chair, there is a lot more to say on the remaining provisions. Due to time constraints, however, I will finish here and would like to refer to the interventions of other civil rights organisations to come as well as to the open letter signed by 79 NGOs from more than 45 countries that raise alarm about the human rights implications of the current draft of the treaty under negotiation.

We hope to continue the discussion on these issues and remain available for further input on the individual provisions during the negotiations.

Thank you.