Eticas Foundation's Oral Intervention on Chapter III, Procedural provisions and law enforcement (2nd round)

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

As held

Thank you Chair,

Honourable Delgations,

Representing Eticas Foundation, we are delighted to be presented this opportunity to share our views on Chapter III of the CND in more detail.

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 serious criminal offences set out in this Convention** (and in our understanding these should only include the offences listed in Cluster 1 of Chapter II, so core cyber-dependent crimes and the standard of serious crimes as explained in my intervention yesterday). 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. More precisely, this means deleting subpara b in para 2.

Also, para 3 should be deleted in its entirety, as Articles 47 and 48 should not become part of the present Convention.

- Article 42: [Conditions and safeguards]

Para 1: The qualifier "applicable" in the first sentence before "international human rights law" should be deleted and no other qualifiers introduced.

Also, a list of references to international human rights treaties should be included in the first sentence after the phrase "under applicable international human rights law". This should be done by including the phrase "including but not limited to the ICCPR, CRC, CAT, and CEDAW and their respective Protocols", as has been suggested and supported by State Representatives.

The reference to the principles of proportionality, necessity and legality and the protection of privacy and personal data should be retained. With regard to the latter, we would like to recall that also at UN level, the General Assembly adopted with consensus a Resolution on the right to privacy in the digital age (Resolution A/RES/77/211, of 15 December 2022).

Para 2 not only requires independent oversight but also prior independent (ideally judicial) authorisation of surveillance measures that interfere with the right to privacy. It should be made clear that the test of legality, necessity and proportionality and the requirements of prior independend (ideally judicial) authorisation and post/ante monitoring apply to all types of personal data, including non-content data (like metadata, traffic data and subscriber information) which is – when aggregated – data of equally highly sensitive nature.

Furthermore, as already stated in our oral statement in the first round of comments on Chapter III which can be found on the website of the Ad Hoc Committee, 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.

● A requirement should be added to ensure that the Convention does **not in any way justify government hacking.**

We would therefore suggest the following addition in **para 1 of Article 42: "Nothing in this Convention shall be understood as obliging State Parties to create a legal basis for the unauthorized access to computer systems of a person of interest or compromise the security of digital communications and services the person of interest is using."**

Article 43: [Expedited preservation of [stored computer data] [accumulated digital information]] As a minimum factual basis it should be added that the expedited preservation is only conducted when „there is a reasonable belief that a criminal offense was committed or is being committed".

Thank you, Chair.