

Eticas Foundation's Oral Intervention on the Zero Draft, Covering Groups 6-10

Delivered by Tanja Fachathaler on behalf of Eticas Foundation

Sixth Session – 21 August to 1 September 2023

Madam Chair,
Excellencies,
Honourable Delegates,

Representing Eticas Foundation, we appreciate the opportunity to once again intervene in the plenary today and I would like to make the following remarks on Group 6 and criminalisation in general. Further comments on Group 9 and 10 I would like to provide at a later stage, once they had been discussed in plenary.

As concerns criminalisation:

First of all, we are pleased to see that many of the controversial provisions of the CND did not make it into the Zero Draft. We very much hope that they will not be included either through an explicit request in this forum or through the backdoor via Article 17.

A narrow scope is key for the successful functioning of the future Convention. Therefore, it should only focus on core cyber-dependent crimes.

• On Group 9 – cyber-dependent crimes:

We would like to draw your attention to the fact that the language on intent required for an act to fall under the criminalising provision is still divergent throughout the text. In most Articles currently a combination of mere „intent“ and „without right“ is required (Arts 7, 8, 9, 10, 11, 12). As pointed out on many occasions in the previous sessions, this still does not protect good-faith hackers (security researchers performing penetration tests) and other groups acting in good faith, such as journalists or human rights defenders.

Also, we urge you to replace the threshold of „dishonest intent“ (Arts 6 para 2, 7 para 2, 11 para 2) with a clearer term such as „criminal intent“, as „dishonest intent“ is too vague and potentially too broad in order to guarantee sufficient protection.

• On Group 10: Protection of personal data

This is a key provision of the Convention and we are of the opinion that the current version in the text which at least in parts builds upon a proposal made in the 5th session by the UK needs further strengthening, as the current text is a somewhat slimmed down version of what was a compromise suggestion back in April. We therefore suggest to at least reinsert in paragraph 2 those parts that have been omitted and that cover explicit data protection safeguards.

These shall be spelled out explicitly, as the term „appropriate safeguards“ is vague and will likely lead to confusion. The safeguards shall include that:

- personal data are processed lawfully and fairly;
- personal data are not processed for a purpose that is incompatible with the purpose for which they were transferred;

- processing is limited to what is relevant and not excessive in relation to the purpose for which the data are processed;
- measures are taken to ensure that personal data that are inaccurate are rectified, marked or erased;
- personal data are kept in identifiable form for no longer than is necessary and appropriate;
- appropriate measures are taken to ensure that the data are protected from accidental or unauthorised destruction, accidental loss or unauthorised access, modification or dissemination; and
- natural persons whose data are transferred are granted enforceable rights, and effective redress.

Madam Chair, these provisions are key to the successful functioning of the future Convention to combat cybercrime while at the same time providing for sufficient safeguards.

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

Thank you.