Derechos Digitales, Electronic Frontier Foundation, Red En Defensa De Los Derechos Digitales, and Eticas Foundation' Oral Intervention on general provisions (agenda item 5)

Delivered By Maria Paz Canales, Derechos Digitales
Fourth Session - 9 January to 20 January 2023

Derechos Digitales, Electronic Frontier Foundation, Eticas Foundation and Red en Defensa de los Derechos Digitales thanks the Chair for her leadership in drafting the consolidated negotiating document and for facilitating the present session.

In drafting the general provisions we would like to recommend the following:

- In Article 1, to limit the purpose of the future treaty to promote and strengthen measures to prevent and combat cybercrime.

- In Article 2, to use the term cybercrime and computer systems, and define it as offences in which computer systems are the direct objects as well as instruments of the crimes, i.e. crimes that could not exist at all without computer systems.

- In Article 3, to limit the scope of application of this Convention to the prevention, detection, investigation, and prosecution of cybercrime as defined; and applies to the collecting, obtaining, preserving, and sharing of evidence in electronic form of cybercrime as defined in the Convention.

- We also recommend that Article 3.3 be deleted completely or reworded. We believe that malicious or fraudulent intent and harm for a violation to occur should be the default rule. Otherwise, trivial violations or even beneficial security or journalistic research can be made criminal. While certain crimes do not need to prove economic or physical harm, for example, interception of private communication, those should be expressed within the definition of that specific crime. As drafted, the wording increases the likelihood of prosecuting individuals for behavior that did not, or could not have been expected to, cause harm or damage.

- We remind States that the principle of sovereignty in Article 4 implies that when conducting an extraterritorial surveillance measure (such as hacking), government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use extraterritorial measures (such as hacking) to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be documented, publicly available, and subject to guarantees of procedural and substantive fairness.

- We value Article 5 on respect for human rights and the inclusion of gender perspectives. However, we note the need to include that specific safeguards be also included in Chapters III and IV of the consolidated text. Failing to reflect these safeguards risks creating a disconnect between the general obligation under Article 5 and those contained in other articles of the Convention — a disconnect that risks creating legal uncertainty and that can be exploited by those governments seeking to justify laws and practices that do not comply with human rights.

We welcome the opportunity to speak today and we look forward to continuing collaborating with the process, and we remain hopeful of having the opportunity to observe Member States' co-faciliated informal discussions this week and the next.