Joint Contribution of Derechos Digitales, R3D, IPANDETEC and Hiperderecho to the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes - Sixth session

Executive Summary

The organizations Derechos Digitales, Red en Defensa de los Derechos Digitales (R3D), Instituto Panamericano de Derecho y Tecnologías (IPANDETEC) and Hiperderecho, belonging to the AlSur consortium of 11 civil society and academic organizations that seek to strengthen human rights in the digital environment, present their proposals regarding the draft text of the Ad Hoc Committee for the elaboration of a comprehensive international convention on combating the criminal misuse of information and communication technologies (A/AC.291/22).

Our recommendations can be summarized as follows:

a) **Gender perspective.**
Digital spaces are inserted in societies affected by pre-existing structural inequalities that can be aggravated and perpetuated by laws and norms. Therefore, it is recommended that the reference to the gender perspective go beyond the Preamble of the document and be incorporated in a cross-cutting manner throughout the Convention and in each of its articles. More specifically, the following changes are recommended: in Articles 24 and 36, the reference to "the need to apply the gender perspective" can be included. In turn, Article 40, have provisions specifying that States have the possibility of refusing a request for legal assistance if there are serious doubts that the request may be based on discrimination based on sex or sexual orientation. In Article 54, reinstate the need to incorporate methods for integrating a gender perspective into policy development, legislation and programming.

b) **Criminalization.**
We welcome the reduction of the catalog of crimes from 30 to 11 offenses, thus focusing on those committed through and against computer systems. However, there are still ambiguities that can criminalize journalistic activities, human rights defense and digital security research. As Latin America is a region that registers an arbitrary use of surveillance technologies and mechanisms of judicial persecution against these groups, it is even more necessary to avoid providing mechanisms that reinforce this situation.
In this regard, we recommend that in Chapter II on criminalization, in Articles 6, 8 and 9, the term "dishonest intent" be replaced by "malicious intent" to reduce the margin of interpretation. It is necessary to evaluate the permanence of Article 10 because it repeats offenses already mentioned in Articles 6 to 9. Another important point in this section is to consider the gender impacts of criminalization on the basis that freedom of expression is essential for gender equality. Legislation that criminalizes the ability

to express social demands related to structural gender inequalities directly undermines their visibility and manifestation.

It is also suggested to establish a legitimate exception in Article 15 on the dissemination of intimate material for the purpose of obtaining evidence and legal advice, since not having it opens the door to re-victimization and criminalization of the victims themselves. It is important that the text eliminates the intention to cause harm as a necessary requirement for this crime and replaces it with "with knowledge of the lack of consent of the victim".

It is also mentioned that the analyzed document includes a new Article (Art. 17) which opens a loophole to criminalize and prosecute actions qualified as crimes in international treaties and protocols when committed through the use of technologies. This is ambiguous and represents a serious infringement on the sovereignty of countries and human rights. The broadness allows the reincorporation of those content crimes that were already eliminated from previous versions of the Convention, for which reason we recommend the elimination of Article 17 in its entirety.

c) Procedural measures

In relation to the procedural measures included in the document, we note several articles. We recommend eliminating paragraphs b and c of Article 23, since they allow the Convention to be applied to other criminal offenses not included in the document itself and allow law enforcement agencies to interfere with the right to freedom of expression by arguing that they are investigating minor offenses.

On the other hand, Article 24 introduces very intrusive surveillance powers, so it is necessary to add a first paragraph establishing principles of legality, proportionality and necessity, as well as the obligation to adequately protect human rights and freedoms.

In Articles 29 and 30, under the same arguments concerning the need to limit the scope of the Convention to prevent it from being used in an abusive or arbitrary manner, we propose to include the reference that these articles shall only apply to the offenses included in Articles 6 to 16 of the Convention.

d) International Cooperation

In Chapter V, We note the lack of safeguards in the powers of mutual legal and technical assistance given to States. It is necessary to add the requirement of dual criminality in Article 35 in order to carry out international cooperation, which ensures that it is not requested for political, gender-based discrimination or other arbitrary reasons. On the other hand, Article 36 only mentions the applicable domestic law on the protection of personal data as an exception for transmitting personal data, which is insufficient since the right to the protection of personal data is internationally recognized and would also harm citizens of countries where the legislation on this matter is not in force. States Parties should not be obliged to transmit personal data if they do not comply with the principles of lawful and fair processing, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

Finally, it is suggested that this Chapter apply a gender perspective in taking into account differentiated impacts with respect to data collection for vulnerable or high-risk communities. It is crucial that data collection, storage and transfer be subject to an intersectional gender analysis to identify the risks to individual security that such procedures entail.