Ad Hoc Committee Sixth Session: Analysis of Draft Text of the Convention

Global Partners Digital submission
August 2023

About Global Partners Digital

Global Partners Digital is a civil society organisation working to ensure that human rights underpin the development, use and governance of digital technologies.

Introduction

We welcome the opportunity to provide comments on the draft text of the convention prepared by the Committee Chair and with the support of the Secretariat.

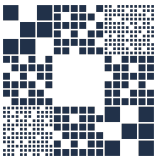
We appreciate the work undertaken so far in the preparation of this document. However, we believe that there are still various elements of the draft text that should be modified to mitigate risks to human rights and ensure the convention is consistent with the states obligations to respect, protect and promote human rights.

Given the nature of the Convention as a multilateral instrument the text should provide a solid common base that represents the best ground to support human rights and democratic principles no matter the particularities of domestic implementation across jurisdictions.

Preamble

We are concerned with paragraph 3 and the reference to offences relating to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing, or and trafficking in firearms, their parts, components and ammunition, drug trafficking and trafficking in cultural property. These bear no reference to the offences included within the treaty and we recommend that they be removed. If illustrative examples are seen as necessary here, we suggest that they only make reference to the crimes contained within the treaty, as opposed to cybercrime more generally.

We are pleased that the preamble makes references to human rights and fundamental freedoms in paragraph 11, and that the text places the respect for human rights as an objective compatible with the pursuing of law enforcement interests. But we believe this provision could better reflect the importance of respect



for human rights. This could be accomplished by removing reference to the need to achieve law enforcement objectives, which is already clear from the other paragraphs in the preamble, and instead focusing solely on human rights. For example, we recommend: "*Ensuring respect for human rights and fundamental freedoms as enshrined in applicable international and regional instruments, particularly the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers*". This modification would provide an explicit recognition of the importance of freedom of expression, as is done with privacy in the following paragraph. This is critical as freedom of expression is, alongside privacy, one of the rights most impacted by cybercrime frameworks, as these can be used to restrict permissible expression online.

Chapter I: General Provisions

- Article 3. Scope of application

We are pleased that the scope of application has been narrowed in article 3(1) to the prevention, investigation and prosecution of the offences established in accordance with articles 6 to 16. However, we strongly believe that the convention should only apply to core cybercrimes as provided for in articles 6 to 10. We would expect that any updates - and ideally further narrowing of offences - would be reflected here as to not capture an overly broad range of criminal activity. For the same reasons we suggest that paragraph 2 should be amended to have the same scope as paragraph 1, avoiding expansion beyond the offences established in the Convention.

- Article 5. Respect for human rights

We are pleased with the continued inclusion of article 5 on respect for human rights, but we believe that this provision could be strengthened by mentioning specific international legal instruments and relevant standards. For example, "*State Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law, including the International Covenant on Civil and Political Rights (ICCPR).*" We further recommend that article 5 make reference to the principles of legality, legitimacy, necessity and proportionality, which are established core principles of international human rights law. The benefit in setting these out within the general provisions is that it reinforces their protective value and application as applying throughout the Convention.

Chapter II: Criminalization

- Articles 6-10 (core cybercrimes)

We welcome that the draft text significantly narrows the scope of criminal offences from previous iterations. We maintain that the scope of criminal offences should be restricted to core cybercrimes - criminal offences in which information and

communications technology (ICT) systems are the direct objects, as well as instruments of the crimes. These currently appear in articles 6-10 of the draft text.

We appreciate that the core cybercrimes in this section must now all be "committed intentionally and without right", but still believe they would benefit from further revision to ensure the intention element reflects a clear and heightened standard to effectively mitigate risks to human rights. For example, we recommend strengthening the requirement around "dishonest intent" but ensuring this terminology is clearly defined within the Convention, or that a more precise formulation of criminal intent is provided.

We welcome that article 6 provides to the states the possibility to request that the offence be committed by infringing security measures, but we will further suggest strengthening this requirement as mandatory rather than optional in order to avoid overcriminalization of conducts for research and other legitimate public interest purposes. Additionally in article 6(2) we suggest deleting "the intent of obtaining" and keeping "dishonest intent" as the intentionality element required for commiting the crime.

We appreciate the language integrated to 10 (2) to avoid the criminalisation of devices use (including programmes, passwords and credentials) in case of testing and protection, but we suggest deleting the reference to "authorized" to avoid public interest security research is unduly limited.

We continue to be concerned that the other articles in this section may capture the legitimate activities such as access to computer systems by journalists, whistleblowers and security researchers and recommend the insertion of a clearly articulated and expansive public interest defence that provides an opportunity for the accused to establish that there was no harm or risk of harm to engaging in the relevant activity, and that the public benefit in the activity outweighed any harm.

- Articles 11-16 (cyber-enabled offences)

While we are convinced that the convention should only include core cybercrimes to minimise potential risks to human rights, we acknowledge that there is potential consensus amongst states that a limited number of cyber-enabled offences should be included. If that is the case, we recommend that these be limited to computer-related forgery and computer-related theft or fraud.

However, without a proper public interest defence as the one suggested in the previous section, article 12 could be interpreted in a way that criminalises the action of whistleblowers and journalists that access information or personal data and share it motivated by public interest or newsworthiness.

We fully agree that combatting and preventing child sexual abuse and exploitation, as well as other forms of online exploitation, are of the highest importance, but still

question the appropriateness of the placement of these offences within a cybercrime treaty.[1] With that being said, if any offences are to be included, we would recommend only article 13 and not articles 14 and 15.

If article 13 is included, it needs to be carefully revised in order to mitigate risks to human rights. For example, we recommend deleting "accessing" in article 13 (1) (b) and "possessing" in article 13 (1) (c), or following the article 20 (i)(f) of the Lanzarote Convention and article 9.4 of Budapest Convention, respectively, considering them optional in order to avoid criminalisation of legitimate actions such as news reporting, victim support or other public interest reasons. The addition of material different from visual depiction enumerated in article 13 (b) risks a negative impact on freedom of expression particularly from the perspective of artistic freedom of representation. We understand that this concern can be partially addressed by the possibility provided to states to limit the provision included in article 13 (3) (b), but we raise that the general provision might result incompatible with freedom of expression restrictions according to article 19 of ICCPR.

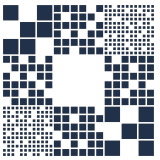
Moreover, we recommend the removal of article 13(2)(a)(iv), which defines child sexual abuse or exploitation material as when it depicts or is implied to be, a victim of torture of cruel, inhuman or degrading treatment or punishment and such material is sexual in nature. This type of material is more adequately addressed in other international instruments and its exclusion would align this provision more closely with the Budapest Convention.

We are pleased that this provision provides protections against the criminalisation of children for self-generated material in article 13(4) and 13(5). However, we believe that article 13(5) could be strengthened by adding "consistent with their obligation under the Convention on the Rights of the Child and its Protocols, as well as with relevant guidance from the Committee of the Rights of the Child."

Again, we do not recommend that article 14 is included. But if it is then we welcome the clearer definition of the offence and the intentionality requested to configure the offence and the clear limitation to adults as perpetrators. However, we suggest reconsidering the language present in the CND in now deleted paragraph 3, "No criminal liability is established if a person has taken reasonable steps to ascertain that the person is not a child", in order to avoid overcriminalization risk created by the inclusion of "communicating" as punished conduct. Otherwise we strongly suggest deleting communicating from the offence.

- Article 17. Offences relating to other international treaties

[1] As others noted in their submissions during the fourth session, 176 states are already party to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which provides for mutual investigative assistance for the offences contained therein. A crime should not be included in the draft treaty simply because it involves the use or commission of technology.



We are seriously concerned by the inclusion of article 17 on offences relating to other international treaties. There is a lack of clarity on which applicable international conventions and protocols are captured by this provision and whether they include those currently in force or those to be established in the future as well. It is also unclear whether this is limited to United Nations treaties. Therefore, we believe that this provision could establish an overly broad scope to the Convention, and introduce duplicative or vague provisions which are not subjected to relevant safeguards established by the Convention and pose risks to human rights. Moreover, we are concerned that this provision could create problems with legal clarity and ultimately hinder efforts to combat cybercrime. Article 17 should therefore be removed from the Convention.

Chapter IV: Procedural Measures and Law Enforcement

- Article 23. Scope of procedural measures

We are very concerned with the scope of procedural measures as set out in Article 23, which provides that the powers and procedures may apply to the criminal offences established in accordance with articles 6 to 16 of this Convention, as well as "(b) Other criminal offences committed by means of [a computer system] [an information and communications technology device]; and (c) the collection of evidence in electronic form of any criminal offence". We recommend that these powers and procedures do not apply to other criminal offences and are limited to the offences established by the Convention and the collection of electronic evidence. This will help ensure that investigatory powers are only used in specific targeted investigations or proceedings with respect to crimes that are consistent with international human rights standards, and further limit the potential for duplicating efforts across the UN system. In the alternative, we suggest at least to amend (b) for referring to "other serious criminal offences".

- Article 24. Conditions and safeguards

We believe that the current formulation of article 24 on conditions and safeguards, is insufficient to mitigate risks to human rights. For example, while we appreciate that the conditions safeguards established under domestic law must be "consistent with its obligations under international human rights law, and which shall incorporate the principle of proportionality" article 24(1) should also make explicit reference to the Universal Declaration of Human Rights, as well as states obligations under international human rights law and customary international law. It should incorporate all relevant human rights principles, including legality, legitimacy, necessity and proportionality. We therefore recommend the following wording: "E*ach State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall be consistent with the Universal Declaration of Human Rights, as well as states obligations under international human rights law and customary international law. This shall*

incorporate all relevant human rights principles, including the principles of legality, legitimacy, necessity and proportionality." This construction is beneficial as it ensures the broadest application of protections with respect to human rights, which is not limited to solely treaty obligations that vary from state to state.

We welcome that article 24 sets out a requirement of judicial or other independent review, grounds justifying application, and the limitation of the scope and duration of such power or procedure. But the current wording is inadequate to ensure protection for human rights. We recommend it be modified to include the following:

- removing the qualifier "as appropriate in view of the nature of the procedure or power concerned" to clarify that the conditions and safeguards expressed in this article apply to all procedures or powers;
- specifying that authorisation requests must be made prior to the procedure execution;
- specifying that authorisation requests must be made by an individual of a specified rank with a competent authority;
- Requiring that any ground justifying the application of such powers shall be based on strong evidentiary showing;
- guaranteeing the right to an effective remedy which provides individuals with the means to challenge measures that impact their privacy;
- including adequate notification of the measure;
- ensuring that any powers or procedures do not compromise the integrity and security of digital communications and services; and
- including reference to the protection of privacy and personal data in paragraph (3).

We recommend that these additional safeguards be included within article 24 to ensure that they apply throughout the chapter, as well as being supported by additional conditions within the specific procedural measures.

- Article 28. Search and seizure of stored data

We recommend removing paragraph 4. We are concerned that the current text can be interpreted as an obligation to weaken or compromise the integrity and security of digital communications and services by demanding the handling of encryption keys or disclosure of security vulnerabilities that enable surveillance.

- Article 29. Real-time collection of traffic data; and Article 30. Interception of content data

We are concerned that various investigative powers, including the real-time collection of traffic data and the interception of content data, contain varying levels of safeguards and conditions. The interception of content data, for example, is only to be provided “in relation to a range of serious criminal offences to be determined

by domestic law", whereas the real-time collection of traffic data is not in relation to a range of serious criminal offences.

We believe that these investigatory powers may pose similar risks to privacy and therefore recommend that they both only apply in relation to the criminal offences established in accordance with articles 6 to 16 of this Convention, or at least to serious criminal offences. Likewise, we suggest that these provisions acknowledge the obligation of state parties to not undermine the security and integrity of digital communications and services posing unjustified risk in the exercise of right to privacy.

Chapter V: International Cooperation

- Article 35. General principles of international cooperation

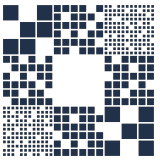
We are concerned that this article does not specify that the powers and procedures provided for in this chapter shall be subject to the conditions and safeguards as provided for in article 24. This is a missed opportunity to mitigate risks to human rights which may stem from international cooperation and we recommend that this language be added.

We strongly suggest that the provisions for international cooperation should only apply in relation to offences contained within the Convention. We therefore recommend that article 35(1) only provides that international cooperation applies in relation to "specific investigations, prosecutions and judicial proceedings concerning offences established in accordance with articles 6 to 16 of this Convention".

We are concerned with article 35(2) as it provides "whenever dual criminality" and instead recommend that the article explicitly note that dual criminality is a necessary requirement. This would ensure that international cooperation is based on the principle that assistance can only be granted if the conduct in question is a criminal offence under the laws of both the requesting and the requested state parties, ensuring that the cooperation granted by the Convention is available for offences that are universally recognized as criminal, avoiding risks of supporting enforcement of crimes that could be incompatible with international human rights law.

- Article 36. Protection of personal data

We welcome the conditions and limitations set out in article 36 with respect to the protection of personal data, particularly those which specify that state parties shall not be required to transfer personal data if it cannot be provided in compliance with their applicable laws. Robust provisions on data protection are essential as they can both safeguard human rights and facilitate international cooperation. However, the provision might be strengthened by referencing directly that personal data transferring conditions should fulfil international human rights standards, not only international law or their respective domestic legal frameworks. It will be useful to



further reference explicitly widely recognised data protection principles such as lawful and fair processing, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

- Article 37. Extradition

We welcome that article 37 provides a number of helpful safeguards:

  - A requirement that the offence is covered by the Convention and criminalised in both states (article 37(1).
  - A requirement that the offence must be punishable by a maximum deprivation of liberty at least of one year (article 37(1).
  - A requirement that any person extradited must be guaranteed "fair treatment at all stages of the proceedings" (article 37(14).
  - Specifying that nothing in this convention shall be interpreted as imposing an obligation to extradite if "the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons" (article 37(15).

These conditions are essential for ensuring the extradition is not used as a tool for political repression. Still, this article can be improved through the following means:

  - Aligning the the dual criminality requirement with the existing provision of UNTOC, namely, providing that "the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party by a maximum deprivation of liberty of at least four years or a more serious penalty".
  - Expanding the requirement that any person extradited must be guaranteed "fair treatment at all stages of the proceedings" to include all the conditions and safeguards contained within the Convention as well as all the rights and guarantees provided by the domestic law and under international human rights law.
  - Specifying that nothing in the Convention shall be interpreted as imposing an obligation to extradite if there are substantial grounds for believing that the person would be in danger of being subjected to torture - as was previously included in the CND.
  - Providing a more open-ended list of grounds under which a state may deny a request for extradition if there are substantial grounds for believing the request was made for the purpose of prosecuting or punishing a person. For example, adding "or other status" within article 37(15). This would provide more comprehensive protection and reflect a deeper understanding of characteristics that could make certain persons or groups more vulnerable.

- Article 40. General principles and procedures relating to mutual legal assistance

We strongly believe that the general principles and procedures relating to mutual legal assistance should only apply to offences within the Convention, or at least only when they constitute a serious crime. However, we welcome that article 40 provides several helpful safeguards:

    - Enabling states to decline assistance when it involves matters of a de minimis nature or on ground of dual criminality (article 40(8); and
    - Enabling states to decline assistance if the requested state party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests (article 40(21)(b).

Still, we recommend that article 40 provide states with the ability to refuse to provide assistance where the offence is "a political offence or an offence connected with a political offence" or where executing the request would likely prejudice, inter alia, "the protection of human rights or fundamental freedoms".

- Article 41. 24/7 network

We suggest the strengthening of this provision by adding language for ensuring the security, reliability, and integrity of the network. All communications shall occur over secure and authenticated channels to safeguard the integrity and confidentiality of the information and avoid access by malicious actors. Law enforcement cooperation should take place in any case within the framework of existing mutual legal assistance treaties, and according to the safeguards established on them, this provision should not provide ground for information sharing outside them.

- Article 42. Expedited preservation of stored [computer data] [digital information] and Article 43. Expedited disclosure of preserved traffic data.

We welcome that articles 42 and 43 are accompanied by several safeguards, including that a request for expedited preservation of stored computer data must specify the offence that is the subject of a criminal investigation or proceedings and the necessity of the preservation (article 42(2). We are pleased that a state may require dual criminality as a condition for responding to a request for mutual assistance for the preservation of stored computer data (article 42(4).

We also appreciate that a request for expedited preservation of stored computer data, and expedited disclosure of preserved traffic data in article 43 may be refused on grounds that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests (article 40(21)(b). Still, we reiterate

the need for both of these articles to contain language that provides the state with broader grounds of refusal due to human rights concerns.

- Article 47. Law enforcement cooperation

We are pleased that article 47(1)(d) does not make reference to the use of illicit encrypted platforms, as suggested in our previous submission of comments to CND and also affirmed by other civil society organisations. We believe the current language is more constructive as it does not risk framing encryption in an overly securitized manner. However, we would recommend strengthening the article by adding reference to the application of the safeguards and conditions established in articles 24 and 36. We also recommend specifying that law enforcement cooperation should be triggered about a specific justified request linked to a committed offence covered in articles 6 to 16 of this Convention. These proposed amendments have the purpose to ensure information exchange is strictly related to the offences covered by the Convention and respects human rights.

- Article 48. Joint investigations

Article 48 on "Joint investigations" should ensure respect for the rule of law, and be modified to avoid its misuse for "forum shopping" or promoting activities that can undermine the protection of human rights. Investigative measures should always be in compliance with the domestic legal framework of the state where the investigation is carried out, or where individuals are targeted, and undertaken in a manner consistent with obligations under international human rights law. We therefore propose to substitute the last sentence of the provision for the following: "State Parties shall ensure that joint investigation teams and their operations are consistent with their domestic legal framework and obligations under international human rights law".

Chapter VI: Preventive Measures

- Article 53. Preventive measures

We are pleased that article 53(2) provides that state parties "shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of individuals, groups and stakeholders outside the public sector, such as non-governmental organisation, civil society organisations, academic institutions and the private sectors, as well as the public in general, in the prevention of the offences covered by this Convention".

This multi stakeholder approach is key to ensuring effective prevention of the offences contained within the Convention. But we believe that paragraph 1 of this provision could be strengthened by making reference to international human rights law, as well as in accordance with fundamental principles of its domestic law.

We also consider that it is important to clearly distinguish preventive measures from criminal procedural measures that could interfere with the rights and freedoms of individuals or legal persons. We therefore recommend adding to the beginning of article 53(3) the following: "These measures should be clearly defined and distinct from criminal procedural measures that could interfere with the rights and freedom of individuals or legal persons. Prevention measures may include:".

Chapter VII: Technical Assistance and Information Exchange

- Article 54. Technical assistance and capacity-building

We believe that article 54 could be improved by making reference to both the domestic legal system and international human rights law. We recommend that article 54(3) be modified to "Activities referred to in paragraphs 1 and 2 of this article may include, to the extent permitted by domestic law and in accordance with international human rights law". We further recommend that technical assistance and capacity-building measures should be subject to human rights impact assessments before they are undertaken, which should provide relevant information on potential risks to human rights and mitigation efforts.

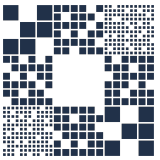
We also believe that article 54(3)(h) could be revised to better reflect a commitment to methods and training in the protection of victims and witnesses who cooperate with judicial authorities, as well as those accused of cybercrime. For example, we recommend the following: "Methods used in the protection of victims and witnesses who cooperate with legal and judicial authorities, as well as those accused themselves of cybercrime, which should include training on trauma-informed and culturally-relevant practices."

- Article 55. Exchange of information

We are pleased that article 55 provides that each state party shall considering analysing, in consultation with relevant experts, including relevant non-governmental organisations, civil society organisations, academic institutions and the private sector, trends in its territory with respect to offences covered by the Convention, as well as the circumstances in which such offences are committed. This demonstrates a clear commitment to addressing cybercrime and better understanding its occurrence through a multi stakeholder approach. However, we believe that this article could explicitly refer to how such trends impact particular groups, including women, children or others. For example, "as well as the circumstances in which such offences are committed and its impacts on particular groups, including as women, children or those persons in vulnerable situations."

Chapter VIII: Mechanism of Implementation

- Article 57. Conference of the States Parties to the Convention



We are pleased that article 57 seeks to establish a Conference of the States Parties to the Convention. We consider this option is preferable to others as we are unconvinced of the viability and long-term effectiveness of a review mechanism or body which sits within an existing UN mechanism. There is a need to ensure that however the conference of parties is shaped, the accessibility and participation from civil society to follow the process can be ensured.

We still believe there is a need to strengthen the language in article 57 to bolster commitments to human rights and safeguard multi stakeholder participation. For example, article 57(5)(e) could be revised to "Reviewing periodically the implementation of this Convention by its States Parties and the impact on the enjoyment of human rights". This should involve seeking input and expertise from existing UN human rights mechanisms on a regular basis. Moreover, the last sentence of article 57(6) should be changed to "Inputs received from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, duly accredited in accordance with procedures to be decided upon by the Conference, will also be considered."

Chapter IX: Final Provisions

- Article 59: Implementation of the Convention

We believe that article 59 should make additional reference to international human rights law. This would reinforce the importance of considering states international human rights law obligations in the implementation of the Convention, as opposed to simply in accordance with its domestic law. For example, article 59(1) could be modified to "Each State Party shall take the necessary measures, including legislative and administrative measures, in accordance with its obligations under international human rights law and the fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention". Moreover, article 59(2) could be modified to "Each State Party may adopt more strict or severe measures than those provided for by this Convention for preventing and combating the offences covered by this Convention if consistent with their obligations under international human rights law". We believe this change would help to mitigate risks of disproportionate measures and sanctions.