NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Fifth Session

11-21 April 2023

Submission of the Office of the United Nations High Commissioner for Human Rights

13 April 2023

1. Introduction

The Office of the United Nations High Commissioner for Human Rights (OHCHR) welcomes the opportunity to provide comments to the Consolidated Negotiating Document (CND) and to continue our participation in the process towards a new Convention. OHCHR reiterates the importance of an inclusive process and the need to put human rights protection at the centre and across all sections of the future UN cybercrime Convention.

OHCHR has consistently called on all parties in the Ad Hoc Committee negotiations to provide the highest level of human rights protection in the future Convention. This includes the way in which the Convention regulates the various forms of international cooperation. In this submission and building on our earlier comments and statements in this process, OHCHR would like to provide a set of observations and recommendations on the sections that are to be discussed during the upcoming fifth round of negotiations, namely: the preamble and chapters on international cooperation (Chapter IV), technical assistance and information exchange (Chapter V), preventive measures (Chapter VI), and mechanism of implementation (Chapter VII).

The approach of the Convention to combat, investigate and prosecute cybercrime, including as part of international cooperation and assistance, entails to a considerable extent measures which provide access to various forms of personal data and which may constitute interference with the right to privacy. As with any interference with the right to privacy, such measures can only be justified when they pursue a legitimate aim, are prescribed by law, and are proportionate to the aim pursued. [1] At the outset, OHCHR

[1] The right to privacy is guaranteed in international human rights law which also sets out the conditions for its restriction, see UDHR Article 12; International Covenant on Civil and Political Rights, article 17; Human Rights Committee, General Comment 16. See also, UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/76/211 (15 December 2022); UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/75/176 (28 December 2020); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, A/HRC/RES/48/4 (7 October 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/73/179 (17 December 2018); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, A/HRC/34/7 (23 March 2017); UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/69/166 (18 December 2014). See also, reports of the High

would like to note two general and inter-related points of caution. First, drafting of certain provisions of the Convention should be further strengthened so as not to allow interpretations that could lead to measures under international cooperation and technical assistance to circumvent or weaken existing safeguards, including safeguards proposed in the draft Convention.[2] Second, successful international cooperation in criminal matters will largely rely on the clarity of the regulatory design, meaning avoiding ambiguity that could lead to fragmented or arbitrary approaches. As it currently stands, several provisions contain undefined, broad and ambiguous terms that would prevent a coherent implementation of the Convention and allow interpretations incompatible with international human rights standards.

The comments offered below are not intended to be exhaustive nor to offer a detailed analysis of each article. Our comments contain observations on human rights considerations arising from the review of the CND's draft articles, in light of international human rights law, including the International Covenant on Civil and Political Rights (ICCPR) and other relevant treaties, as well as relevant jurisprudence. The comments focus on some of the most relevant issues from a human rights perspective.

2. Preamble

OHCHR recommends that the broad assertions in the preamble, such as those suggesting a causal link between cybercrime and other issues, be narrowed and included only where a strong factual basis is established.

In addition to the preamble's many references to the threats posed by cybercrime, OHCHR believes that the preamble can be made more nuanced and complete by equally acknowledging that certain existing measures to combat, investigate and prosecute cybercrime often disregard or do not sufficiently take account of their human rights implications, including on the rights to privacy,[3] due process and fair trial.

Furthermore, OHCHR notes that the sole existing reference to human rights in the preamble could lead to misinterpretations. The wording "ensure a proper balance" between the interests of law enforcement and respect for human rights suggests a dichotomy between law enforcement and human rights. However, law enforcement itself is subject to constraints under international human rights law, and human rights law – far from preventing law enforcement measures – establishes conditions under which law enforcement measures should be carried out. It is widely acknowledged that respect for human rights by law enforcement enhances effectiveness,[4] including in solving and preventing crime. In this sense, human rights compliance by law enforcement, in addition to being a legal imperative, enhances performance and results. In other words, there is no

Commissioner for Human Rights and the Office of the High Commissioner for Human Rights, "The right to privacy in the digital age", A/HRC/51/17; A/HRC/48/31; A/HRC/39/29; A/HRC/27/37.

[2] See report of the Office of the High Commissioner for Human Rights, "The right to privacy in the digital age", A//HRC/39/29, paras. 21-22, highlighting human rights risks in the context of international cooperation and information sharing in the absence of sufficient safeguards.

[3] International Covenant on Civil and Political Rights, article 17; Human Rights Committee, General Comment 16; Report of the Office of the High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/51/17

[4] See Office of the High Commissioner for Human Rights, "Human Rights and Law Enforcement", Professional Training Series No.5/Add.2 (2002).

balancing needed between law enforcement and human rights. OHCHR therefore recommends this wording be amended.

OHCHR would like to recommend a clearer recognition of international human rights law, including in the context of law enforcement, investigation measures and international cooperation. For example, the following language could be added

> "*stressing that any measures to combat, investigate and prosecute cybercrime must be consistent with applicable international law, including international human rights law and standards, in particular the rights to privacy, due process and a fair trial. Any interference with the right to privacy resulting from the application of this Convention must be non-discriminatory, pursue a legitimate aim, be provided by law, and be necessary and proportional."* [5]

3. Scope of international cooperation and technical assistance

International cooperation in criminal matters significantly relies on national design of regulation and enforcement of national law. The importance that is attached to international criminal justice cooperation depends on how much of a threat cybercrime is perceived to be, and on the resolve to counter such threats. International cooperation depends on building trust, which can be built through a framework for international cooperation that is transparent and gives clear parameters for the exchange of information and evidence.

OHCHR recommends that the scope for international cooperation be limited to criminal offences as set out in the Convention. To the extent that the scope is broadened for the collection of electronic evidence in relation to other criminal offences, OHCHR recommends that this be specifically defined under the Convention and limited to "serious criminal offences", defined as "criminal offences causing death or serious bodily harm".[6] While acknowledging the difficulty in defining "serious criminal offences", OHCHR believes the suggested definition could constitute a reasonable limitation that would assist in avoiding arbitrariness in the way in which international cooperation is conducted. There should be opt-out clauses for the purpose of ensuring compliance with human rights safeguards and based on domestic legal frameworks.[7]

OHCHR reiterates its earlier comments that the conditions and safeguards in the procedural and law enforcement provisions under Chapter III are equally relevant in the context of international cooperation and legal assistance. OHCHR therefore welcomes the explicit reference of article 56(4) to article 42 (*Conditions and safeguards*). OHCHR reiterates its comments on article 42 submitted in writing on 19 January 2023[8] and in its

[5] Ibid.

[6] By comparison, the United Nations Convention on Transnational Organized Crime (UNTOC) uses the term "serious crime", defined as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty" (UNTOC, article 2b). However, in view of significant variations between jurisdictions concerning both the type of acts that are criminalized and their penalty, OHCHR believes that a definition based on the duration of the penalty could hinder meaningful international cooperation. In comparison, the International Covenant on Civil and Political Rights (ICCPR), article 6, uses the term "most serious crimes", interpreted by the Human Rights Committee in General Comment 36, para. 35 as "intentional killing" (CCPR/C/GC/36, para. 35).

[7] In line with the International Covenant on Civil and Political Rights, article 2.

[8] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf.

oral statement of 18 January 2018.[9] Article 42 is central to mitigating the risk of human rights violations and abuses. In order to ensure consistent application and an adequate level of human rights protections, the provision could be strengthened and made clearer by completing the list of minimum safeguards that should be applicable to the procedures and powers provided under the Convention. OHCHR would like to suggest the following language for article 42:

> "1. *Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for under the Convention are in compliance with international human rights law, including the right to privacy and the protection of personal data. All those powers and procedures shall be carried out in accordance with international law, including international human rights law and taking into account the gravity of the crime concerned and the nature of the procedure or power concerned.*
> *2. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for under the Convention are subject to adequate conditions and safeguards, including judicial or other independent supervision, prior judicial or other independent approval, grounds justifying application, limitation of the scope and the duration of such power or procedure, adequate notification, access to remedies, and confidentiality of attorney-client and other privileged communications.*
> *3. Independent oversight bodies shall have the authority to conduct audits, spot checks and impose redress measures.*
> *4. Each Party shall consider the impact of the powers and procedures in this Convention upon the rights and legitimate interests of third parties."*

OHCHR also recommends that article 75 (*Law enforcement cooperation*) make explicit reference to the need for cooperation to be conducted in accordance with international human rights law and safeguards. For example, a suggested formulation for article 75(1) could be:

> "*States Parties shall cooperate closely with one another to combat the offences covered by this Convention, consistent with their respective domestic legal and administrative systems, international human rights law and this Convention,".*

Furthermore, OHCHR recommends the removal of the verbs "preventing" and "disrupting" from article 56(1), as these terms could open up the scope of the Convention to expansive interpretations and measures.

International cooperation should ensure that States respond to legal assistance requests in a manner consistent with international human rights law. The exchange of and access to data entails human right risks, particularly concerning privacy, and requires robust safeguards to ensure that neither the State is given too large of a leeway, nor that the private sector is coerced into sharing data in ways that may be contrary to international human rights law, including putting individuals at risk, or for purposes that are outside of the scope of the Convention. OHCHR believes that the Convention should strictly uphold

---

9 https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Statements/OHCHR_statement_on_procedural_measures_for_upload.pdf.

privacy protections, including in the context of international cooperation and mutual legal assistance. At a minimum, cross-border cooperation measures that interfere with the right to privacy should be conditioned on the existence of a level of privacy and data protection in the requested State that conforms with internationally recognized minimum standards.[10]

In the context of technical assistance, including as set out in article 87, OHCHR recommends specifically highlighting that technical assistance be directed at increasing capacity of law enforcement alongside judicial systems not simply for the purpose of capacity building in technical matters but equally for the purpose of upholding the rule of law . The Convention should consider building capacity for States in a fully transparent way, with attention to how safeguards against overreach by law enforcement and other authorities can be built into assistance provided between States Parties.

Moreover, OHCHR notes the draft's many references to States Parties affording each other "the widest measure" of cooperation or technical assistance (see for example articles 61(1); 79; 87(1)) or references to "maximize the effectiveness" of various forms of cooperation or assistance (see for example preamble and articles 75; 87(6); 89(2)). OHCHR reiterates previously submitted comments that such language, in the absence of clear human rights safeguards in the Convention, inappropriately requires States to pursue law enforcement and other measures without taking into account the human rights affected by such measures. OHCHR recommends replacing such formulations with language requiring any cooperation or measure to be consistent with international human rights law.

4. Safeguards: Recommendations on substantive elements

A. Grounds for refusing international cooperation

OHCHR recommends the inclusion of general and mandatory clauses for refusal of international cooperation and legal assistance in addition to clauses that can be left at the discretion of the States Parties.

Dual criminality

OHCHR welcomes the mandatory requirement of dual criminality found in article 61(6) in the context of extradition. Such a requirement is in line with the principle of dual criminality enshrined in the UN Convention against Transnational Organized Crime.[11]

On the other hand, OHCHR notes that dual criminality is set as a discretionary option, instead of mandatory, in article 68(3) concerning preservation of stored data, as this also seems to be inconsistent with article 68(4). Beyond extradition, as a matter of human rights policy, OHCHR recommends the inclusion of a general dual criminality requirement for all international cooperation and assistance, requiring that the alleged criminal offence for which international cooperation is being sought must be criminal in both the demanding and the requested States Parties. Such a clause would itself be a safeguard which could help ensure that international cooperation is carried out for the purpose of the criminal offences as set out in the Convention or for serious crimes, thereby

[10] See A/HRC/39/29, paras. 27-33, outlining such standards.
[11] See also, article 16(1).

preventing the use of the Convention for the pursuit of other objectives, which may be incompatible with international human rights law and standards. .

Political offences objection clause and refusal on the basis of human rights

In line with international human rights law, OHCHR welcomes the inclusion in articles 68(5)(a) and 69(2)(a) of a clause allowing the refusal of disclosure of traffic data or preserved data as part of mutual legal assistance if the request concerns an offence considered a political offence, or an offence connected with a political offence, in the requested State. OHCHR recommends that such clauses are made general so as to apply not only to cases of mutual legal assistance on data preservation and disclosure of traffic data, but to any cooperation and legal assistance.

OHCHR notes that article 58(4) *in fine*, states that "*A State Party whose law so permits, in case it uses this Convention as the basis for extradition, shall not consider any of the offences established in accordance with this Convention to be political offences".* The provision clarifies that offences under the Convention shall not be deemed political offences. Yet, OHCHR notes the risk that such a provision may be misinterpreted to permit extradition even in cases where the individual in question formally is prosecuted for an offense under the Convention, but where the prosecution either pursues ulterior motives or is otherwise based on conduct which would qualify as a political offence.

While article 58(15) contains welcome language on grounds for the refusal of extradition. OHCHR expresses strong concerns that the provision in question is more restrictive than the obligations of States to refuse extradition under applicable international law, including international human rights law. There thus appears to be a real risk that the application of the Convention with the proposed wording of article 58 (15) would include situations that may amount to violations of international human rights law.

OHCHR notes, for example, the exhaustive list of prohibited grounds of discrimination, the absence of a general reference to international human rights law, including the right to life and the prohibition of arbitrary deprivation of liberty, and the absence of a general reference to the principle of non-*refoulement*.

As such, we recommend deletion of the above language at the end of article 58(4), along with the inclusion of the following general and mandatory clause for refusal:

> "*Extradition shall be refused if the extradition would be contrary to applicable international law, including international human rights law, or if it concerns an offence that the requested State Party considers a political offence or an offence connected with a political offence.*

OHCHR further recommends adding a clause requiring authorities in the requested State to take into account the following factors as part of their proportionality test when considering extradition requests: i) the seriousness of the offence (for example the harm or danger it has caused); ii) the likely penalty imposed if the person is found guilty of the alleged offence; iii) the likelihood of detention; and iv) the interests of the victims of the offence.

Beyond the situations of extradition and requests for disclosure of traffic data or preserved data, OHCHR recommends the inclusion of a general clause for refusal of international cooperation and mutual legal assistance, in situations where the requested State party has reasonable grounds to believe that there is a high risk that its cooperation may result in violation of human rights by the requiring State Party, including procedural rights. Such a clause can be merged with a general clause on refusal based on prejudice to sovereignty, security, *ordre public* or other essential interests, that is currently found in several articles, such as articles 61(19); 68(5)(b); 69(2)(b). For example, a general clause could establish that:

> "*International cooperation and mutual legal assistance shall be refused if (a) there are reasonable grounds to believe that the criminal offence will be treated as a political offence by the requesting State; (b) there are reasonable grounds to believe that the cooperation or assistance will result in a violation of human rights; (c) the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or other proceedings under their own jurisdiction;*
>
> *International cooperation and mutual legal assistance may be refused if the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, or ordre public."*

Such a clause would be an important safeguard for situations where article 42 is not sufficiently specific.

In the context of extradition, OHCHR would like to refer to two formulations in article 58. Firstly, article 58(9) requires States to "simplify evidentiary requirement" for the purpose of the offence forming the ground for extradition. Secondly, article 58(11) provides that domestic prosecution of a case which could be but is not subject of an extradition, should be undertaken as any other "offence of a grave nature under domestic law". OHCHR notes that such broad and ambiguous formulations risk to be interpreted in way that undermine or are incompatible with the rights of due process and fair trial..

B. Specific safeguards in the conduct of cooperation measures

Prior authorization

OHCHR notes that as the draft currently stands, there is no explicit requirement of prior authorization of procedural measures or retroactive review by an independent body, ideally a judicial one. As earlier submitted, independent authorization is a key safeguard for privacy-intrusive procedural measures, including in the context of measures undertaken as part of international cooperation. As article 56(4) subjects the procedures and powers in the chapter on international cooperation to the conditions and safeguards provided in article 42, OHCHR reiterates its recommendation to include a specific reference in article 42 to the need for prior judicial authorization as well as independent oversight over the measures carried out under the Convention. Such authorization should be a mandatory safeguard at least for covert procedural measures (where the suspect is not aware of the measure), with exceptions only allowed in acute time sensitive circumstances and in any event requiring subsequent independent review within strict

timeframes. As such it would apply to intrusive measures in the context of international cooperation and mutual legal assistance, such as collection of real-time traffic data and accessing, seizing, or securing data in articles 70-74.

Safeguards in the context of transfer of personal data

Article 57 provides for the transmission of personal data from one State Party to another. OHCHR welcomes the inclusion of language aimed at establishing necessity and proportionality requirements. OHCHR believes that this provision could be strengthened to make these requirements more precise by adding language strictly limiting the transmission of data to the initial criminal proceedings for which the request was made or for the prevention of imminent and serious threat defined as threat to life or safety of people.

In this connection, OHCHR notes that article 57(1) does not refer to serious threats to life or safety of people in general, but about only to "*serious threat to the public safety of those persons whose personal data are transmitted".* OHCHR recommends that the language be amended so as to reflect the safety of people in general, not limited to "public safety" and not limited to "people whose personal data are transmitted".

Furthermore, article 57(2) should require the requesting State Party to provide a justification for the time duration for which it is requesting the data. Currently, the only condition in the text for extending the time period is a request from the requesting State Party. OHCHR recommends that this be amended to include a requirement that the request includes a justification for why an extension is sought and how the extension is necessary for the purpose for which it is sought.

OHCHR would like to highlight that, as a general rule, the individuals whose data are concerned should be notified about the transfers.[12] Exceptions should be construed narrowly, for situations where disclosure would pose a real and foreseeable risk to an ongoing investigation.

OHCHR would also like to note that while article 57 is called "protection of personal data", there is limited language on measures required to adequately protect personal data. OHCHR recommends the inclusion of a general requirement for ensuring that data protection laws exist and are enforced in the receiving State Party, and meet at least minimum human rights-based standards.[13] Moreover, in order to avoid that article 57 could be interpreted and applied in a way that could undermine already existing data protection levels, OHCHR also recommends that it should expressly be clarified that the article is without prejudice to, and should not be understood to restrict or limit, existing data protection frameworks regulating cross-border data transfers.

[12] Under international human rights law requirements of transparency and the associated necessity to notify are key elements of the rights to an effective remedy and may also impact on the right to fair trial. It would not be possible for a person to effectively challenge a government's interference with her or his privacy without knowing whether she or he has been subject to interference with the right to privacy in the first place. The right to fair trial is guaranteed under article 14 of the International Covenant on Civil and Political Rights and the right to effective remedy is guaranteed in article 2(3) of the International Covenant on Civil and Political Rights.

[13] See A/HRC/39/29, paras 27-33 outlining such standards.

Finally, article 57(5) conditions the sharing of personal data with third parties on either the consent of the State Party transmitting the data or of the person concerned. The Convention should ensure that such transfers to third parties are conditioned on strict requirements and strong safeguards, such as adequate data protection levels, including purpose specification and limitation, data minimization and time limits.

Specification of the criminal offence for which data is sought

Several provisions allow for access to data, preservation, and other measures, for the purpose of criminal investigations or proceedings, with requirements for what the request should include (see for example, articles 61(14); 68(2)(b); 73(3). OHCHR notes that such clauses require additional specifications to meet minimum safeguards under international human rights law and standards, including the principles of non-discrimination, legality, proportionality and necessity. OHCHR recommends that such clauses be enhanced to add a requirement of "reasonable grounds to believe that a criminal offence as established under the Convention or a serious crime is committed or about to be committed" which is subject of a criminal investigation or proceeding. Moreover, the criminal offence for which data is sought should be provided as well as a justification about how the measure is necessary and proportionate to the investigation or proceeding.

In the context of preventive measures, article 93 provides overbroad language for access to information about individuals from financial institutions and organizations, but without sufficient safeguards. For example, the provision allows for information about identity of individuals "*where there is information regarding their possible involvement, or the possible involvement of members of their families or close associates or persons acting on their behalf, in the commission of offences established in accordance with this Convention, including information on the accounts of all the above-mentioned persons".* OHCHR recommends to include safeguards requiring reasonable grounds to believe a criminal offence covered by the Convention has been or is being committed, and to limit the scope of people whose information can be obtained to those directly associated with the criminal offence.

Compliance with domestic law, procedures and safeguards

Certain provisions allow for measures under international cooperation and mutual assistance to the extent that they would be "available in a similar domestic case" (see articles 61(4)(e); 73(2)) or "not contrary to domestic law" (see article 61(16)). OHCHR recommends that these formulations be enhanced to require they be "authorized under domestic law and in line with domestic law, procedures and safeguards".

Strengthened consent requirement for access to cross-border stored data

Article 72(b) conditions cross-border access to stored data, without the authorization of the State Party in which the data is stored, on whether the requesting State Party obtains the "lawful and voluntary consent of the person who has the lawful authority to disclose" the data. The wording "lawful authority" could support a problematic interpretation, according to which service providers could release information about their users, for example on the basis of their own terms of service granting them the right to do so. To clarify that consent shall not be considered valid if provided by a service provider on behalf of an individual user, OHCHR recommends amending the language to require

"*lawful and voluntary consent of the person whose data is disclosed",* to prevent giving service providers the authority to hand over data on the basis of broad terms of service.

Notification

Article 68(2)(g) allows for confidentiality of requests for data preservation as a default. However, being informed of rights-restrictive measures is a prerequisite for access to remedy.[14] It is moreover needed for accountability and building public confidence in law enforcement measures. Consequently, confidentiality obligations should be limited to the extent necessary to protect legitimate criminal investigations or other protected interests. Therefore, OHCHR recommends amending this provision to clarify that confidentiality has to be justified in each case. This could be done by adding at the end of the provision the phrase "because there are reasonable grounds to believe that the disclosure of the request would imperil the ongoing investigation or would cause death, serious bodily injury or other serious harm."

Time limitations

Article 68(7) provides for a minimum period of sixty days for data preservation, with a possibility for unlimited extension following a request from a State Party. Similarly, article 57(2) does not provide any maximum time for the holding of transferred data. Given that in their current form these articles also fail to provide adequate safeguards, the absence of time limitations, could result in undermining the enjoyment of human rights . OHCHR recommends the provisions be amended so as to establish a maximum period for data preservation, with a possibility for time-limited extension following a request from the requesting State Party justifying the necessity for the extended period of data preservation.

Mutual legal assistance in accessing stored data

Article 70 concerns requests to access, seize, secure and disclose stored data pursuant to article 68. Yet, this provision fails to include safeguards as found in other provisions concerning mutual legal assistance. In the absence of any safeguards in the article, there is a possibility for wide-ranging access to any kind of data. As noted in OHCHR's submission to the Ad Hoc Committee of 17 January 2022, personal electronic devices frequently contain highly sensitive personal information not only about their user/owner, but also many third parties. Search and seizure measures regarding such devices therefore can carry even greater risk to human rights, including the right to privacy, than covert access to data on a particular individual. It is thus essential that the future Convention ensures that these measures are subject to sufficient independent oversight and control. OHCHR therefore recommend amending language to that effect that includes minimum safeguards, including requiring that a request for access to stored data provides information about reasonable grounds that a criminal offence as established under the Convention is committed or about to be committed; information about how the stored data is necessary for criminal investigation or proceedings directly related to the offence, an explanation that the data sought is relevant for such investigation/proceedings, and subject to sufficient independent oversight and control.

[14] See report of the Office of the High Commissioner for Human Rights, "Privacy in the Digital Age", A/HRC/39/29 para 54.

Review through civil society participation

OHCHR welcomes that article 92 requires from States Parties to promote the active participation of individuals and groups outside the public sector, including non-governmental organizations, academia, community-based organizations, and the private sector, in prevention efforts. To complete the range of topics where contributions of civil society groups would be of great value, OHCHR recommends adding language about the evaluation on any adverse impact on human rights as a result of the implementation of measures under the Convention. It is important not only to provide safeguards in the law and regulations governing matters under the Convention, but also to carry out ongoing checks to see if these safeguards work in practice. Public oversight also requires governments to release sufficient and clear information to the public to allow for a serious assessment of the necessity and proportionality of the measures under the Convention in practice.

C. Mechanism for implementation

OHCHR recommends that the Convention not only draw on the experience of existing implementation and review mechanisms of UN treaties but does so with the purpose of improvement in line with the development of international standards on transparency and participation. Moreover, the Convention should use the opportunity to put human rights compliance clearly within the realm of the implementation and review mechanisms.
In particular, OHCHR recommends that a future provision on a periodic review of the implementation of the Convention establish that the review should include the impacts on the enjoyment of human rights (see the current proposals for article 95(4)(e)).
OHCHR further recommends inclusion of UN human rights mechanisms in the review of the implementation of the Convention, and for States to use the Universal Periodic Review process to include relevant issues pertaining to the rights implicated under the Convention.

As a step to achieve this, OHCHR would like to recommend the establishment of a body of independent experts to monitor the implementation of the Convention, with capacity to consider the human rights issues relevant to the Convention including through seeking input and expertise from existing UN human rights mechanisms.

OHCHR notes that there is currently only a very limited reference to cooperation with civil society organizations for the purpose of implementation. This reference is contained in article 95(4)(c) and is limited to "relevant (…) non-governmental organizations". OHCHR underlines that any successful implementation of a Convention and its review, including the delivery of effective and efficient capacity building and technical assistance, relies on the participation of civil society and other non-governmental actors. OHCHR strongly recommends enhancing the provisions on both implementation and review of implementation to facilitate the active and inclusive participation of civil society, academia and the private sector. This recommendation applies to all review mechanisms, including the proposal for an International Technical Commission (article 95bis), which in its current form would exclusively consist of State representatives, missing a key opportunity to benefit from insights from a broad range of stakeholders and experts.

D. Recommendations for provisions to be deleted

In addition to the points made earlier in this submission, OHCHR would like to flag provisions that we consider to be particularly problematic from a human rights perspective. We suggest them to be either significantly amended or otherwise deleted. These include the following:

Article 64: Spontaneous information

Article 64 allows, under certain conditions, a State to proactively share information with another State. While there can be compelling reasons for permitting voluntary sharing of information, there are currently no safeguards included in the article to ensure that such information is obtained in ways that are compatible with international human rights law. For example, a State could obtain information through intrusive measures and transmit such information voluntarily to another State, without any possibility for the receiving State to assess the human rights implications of the methods used. This concern is aggravated by article 64(2) which allows for keeping the information confidential. Overall, by establishing a legal basis for so-called spontaneous information sharing without providing an adequate set of safeguards risks inviting the circumvention of the conditions and safeguards applicable to other forms of cooperation. OHCHR therefore recommends either adding safeguards that can ensure that the information is obtained in ways that are authorized and in line with domestic law, safeguards and procedures, or otherwise deleting the article.

Article 75(1)(d)

This article requires the adoption of mandatory measures to exchange information on "*the use of illicit encrypted platforms and [cybercrime tactics, techniques and procedures] [tactics, techniques and procedures associated with the use of information and communications technologies for criminal purposes], as well as operational indicators of compromise"*. The wording is broad and vague (i.e. "operational indicators of compromise") and is also formulated in a way that suggests, contrary to international human rights law, that encrypted platforms are illicit. OHCHR recommends the deletion of this part of the article.

Article 76: Public-private partnerships to enhance the investigation of [cybercrime] [the use of information and communications technologies for criminal purposes]

This provision is overly broad and lacks safeguards. The article opens the possibility of privatization or outsourcing of public responsibilities that involve the collection and processing of personal data. Any public-private partnership would require detailed safeguards to ensure compliance with international human rights law that would have to go beyond the broadly phrased mechanisms recognized under article 42. OHCHR recommends the deletion of this article.

Article 78: Special investigative techniques

Article 78 is vague and overly broad and would allow for intrusive measures, with the only limitation being compliance with domestic law. As such, it introduces broad measures without protection from arbitrary interference. The notion "special investigative techniques" creates an opportunity for the use of any surveillance technique, including

those that may be prohibited under international human rights law, such as government hacking. As such, it fails to comply with the requirements of legality, necessity and proportionality under international human rights law. OHCHR further notes that the language in article 78(4) appears to be inspired by article 20 of the United Nations Convention against Transnational Organized Crime (UNTOC) which is concerned with the interception of goods. That, however, is an entirely different context, which may necessitate measures aimed at "removal or replacement". However, such language is unsuitable when we speak about data. OHCHR therefore recommends deletion of this language.