Photos by Unsplash: Camilo Jimenez

INFORMATION NOTE

Human rights and the draft Cybercrime Convention

INTRODUCTION

OHCHR supports the process of elaboration a new convention addressing the threat of cybercrime and the need for better cooperation in collecting electronic evidence across borders. It encourages States to agree a text that complies fully with international law, including International Human Rights Law.

By firmly grounding the new Convention in existing international human rights law, the Convention will effectively contribute to addressing cybercrime in accordance with the principles of legality, due process and the rule of law. A failure to do so would not only undermine efforts to address cybercrime but also contribute to an environment that enables it.

This information note identifies key human rights messages for treaty drafters, civil society organizations and other stakeholders based on the revised draft text of the Convention of May 2024. In focusing on key messages, the briefer does not exclude stronger human rights-related provisions that Member States and other stakeholders might propose.

1 A/AC.291/22/Rev.3.

It should be noted that each of the areas highlighted below raises specific concerns from the perspective of international human rights law, each warranting close and separate consideration. In this regard, OHCHR cautions against compromise positions that might concede a lower standard in some of these areas as part of a broader package.

KEY MESSAGES

OHCHR recommends:

- Explicit references to relevant human rights treaties
- Explicit provision to clarify that nothing in the Cybercrime Convention should be interpreted as impairing or reducing the scope of States' obligations under international human rights law
- Inclusion of a general safeguards clause to ensure that States implement the obligations under the Cybercrime Convention in compliance with their obligations under international human rights law
- Precise and narrow scope of criminal offences subject to the Cybercrime Convention that avoids criminalizing acts that enjoy protection under international human rights law, such as the exercise of freedom of expression
- Clear protection of the rights of the child, in compliance with the Convention on the Rights of the Child
- Clear provisions to avoid the misuse of procedural measures so as to protect the right to privacy and other rights
- Formulation of provisions on international cooperation and mutual legal assistance that avoid any possible conflicts with States obligations under international human rights law.

REFERENCES TO HUMAN RIGHTS

OHCHR welcomes references to human rights in the current preamble and draft article on 'Respect for human rights' (preamble, articles 6 and 24 of the draft text).

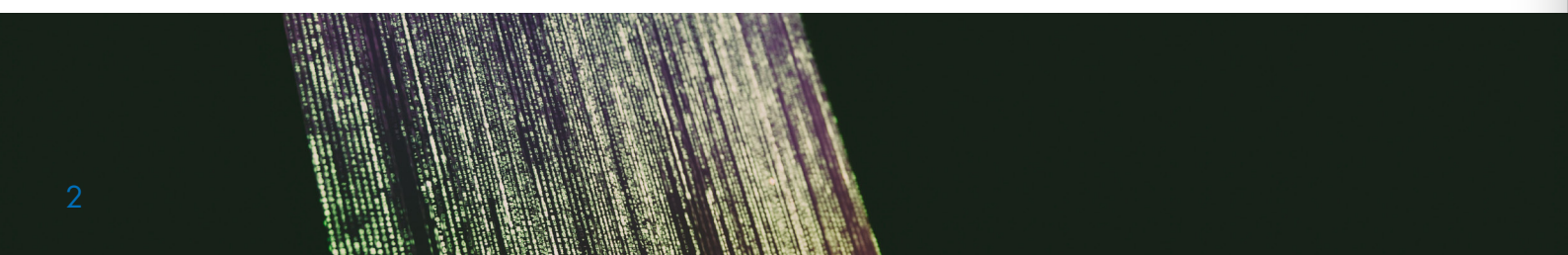
WHY ARE EXPLICIT HUMAN RIGHTS REFERENCES IN THE CYBERCRIME CONVENTION IMPORTANT?

The complex reality of investigation and prosecution of crime, including cybercrime, requires safeguards to prevent arbitrary interference with individual rights, such as the right to privacy and the right to liberty and security of person, and requires full respect for due process of law and fair trial protections. Explicit human rights references in the Cybercrime Convention will leave no doubt as to the imperative to respect these safeguards in the exercise of States' legal authority in relation to individuals when implementing the Cybercrime Convention. Moreover, against the background of frequent abuse of cybercrime laws, it is important to ensure that the Convention explicitly clarifies that it does not cover such acts. OHCHR therefore welcomes the inclusion of article 6(2) clarifying that the Convention cannot be used to justify repression.

CRIMINALIZATION

Chapter II of the draft text sets out the scope of criminal offences that would be subject to the Cybercrime Convention's provisions. OHCHR highlights the importance that the scope of criminalization should be precisely and narrowly defined in order to avoid ambiguities that could threaten legitimate activities, including activities pursued in the exercise of human rights. This would help ensure consistency of the Convention with International Human Rights Law and comply with the principle of legal certainty.

Photos by Unsplash: Shahadat Rahman



KEY MESSAGES

OHCHR recommends:

- Deletion of article 4
- Explicit inclusion of the existence of criminal intent and consequential harm as conditions for criminalization of conduct covered by the convention in articles 6-11
- Explicit mandatory exclusion of the criminalization of children for posting self-generated material on-line.
- Explicit exception for artistic, educational and scientific material in relation to the term 'child sexual abuse material'
- Protection of individuals below the age of 18 whose images are shared without their consent

NARROW V BROADER SCOPE

OHCHR encourages limiting the scope of the Convention to the criminalization of certain cyber-dependent crimes – in other words, offences that are inherently linked to computer data or systems. Article 7 provides an example of such a crime in the form of intentional access to a computer system without a right.

Broadening the scope of criminalization beyond cyber-dependent crimes could be problematic, in particular if offences based on the content of online expression were included. Cybercrime laws with such provisions are frequently used to unduly restrict free expression, suppress political dissent, and are often weaponized against minorities. An example of a broader scope of criminalization would be the inclusion of the criminalization of 'terrorism' in the Convention, where such an act has occurred using a computer system although not dependent on a computer system. The open and ill-defined nature of 'terrorism' could be used to apply the provisions of the Convention to criminalize acts that might in fact be considered legitimate criticism of the State or a powerful actor, in keeping with the right to freedom of expression, using the Cybercrime Convention as a justification for criminalization.

Against this background, OHCHR notes with concern the new suggested title of the Convention "United Nations Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System)". This could be read as defining any criminal act done via an ICT system as cybercrime. Such an approach would be particularly problematic against the background of article 1 that defines the purposes of the Convention as combatting and preventing "cybercrime". Read together with the title, this could lead to an expansive interpretation of the purposes that would contradict the attempts at limiting the scope of criminalization under the Convention to clearly and narrowly defined offences.

In this regard, OHCHR remains concerned about the open-ended nature of article 4 (formerly article 17). Article 4, now at a very prominent place in the draft Convention, requires States to adopt measures to broaden the Convention's coverage to offences under other international instruments when committed through the use of a computer system. The actual scope of this provision is not clear, for lack of an exhaustive list of relevant offences, and consequently, it is currently not possible to assess its future impacts. It risks expanding problems experienced in the application of other treaties, for example with regard to overly broad definitions of terrorism. The provision could also lead to establishing disproportionate liability regimes for service providers, which in turn would threaten the right to freedom of expression. Deletion of article 4 would help to ensure a narrow scope and clear application of the Convention.

Finally, plans for an additional optional protocol to cover additional criminal offences carry the significant risk for an expansion of criminalization that would not meet the requirements of international human rights law, including the principles of necessity and proportionality.

EXPLICIT INCLUSION OF CRIMINAL INTENT

The scope of the Convention should avoid covering acts performed without criminal intent. For example, articles 7 to 11 may, in their current form, be applied to criminalizing common practices, such as the disclosure of information for the purpose of revealing illegal activity,

fraud or acting for the purpose of protecting a general public interest, for example activities of independent cybersecurity researchers.

Articles 7 -12 currently allow States the discretion to subject offences to a requirement of dishonest or criminal intent. Such requirements should instead be mandatory rather than discretionary, so as to protect legitimate acts that have not been committed with criminal intent.

OHCHR proposes the following amendment for article 7.

- *Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed ~~intentionally~~* ***with dishonest or criminal intent****, the access to the whole or any part of an information and communications technology system without right.*

- *A State Party may require that the offence be committed by infringing security measures, ~~with the intent of obtaining electronic data or other dishonest or criminal intent~~ or in relation to an information and communications technology system that is connected to another information and communications technology system.*

Articles 8-10 and 12 should also be changed in a similar way.

Should it prove difficult to agree changes to the articles themselves, in particular against the background of difficulties in finding appropriate language to describe the elevated intent that should be required, an interpretative note could provide additional clarity.

MANDATORY EXCLUSION OF THE CRIMINALIZATION OF CHILDREN

Protection of children from sexual abuse is of utmost importance and required by international human rights law. At the same time, international human rights law protects the freedom of expression of children.

Consequently, while the criminalization of cyber-related acts of sexual abuse of children is justified, such crimes should be formulated with precision, and avoid the criminalization of legitimate expressions, including the sharing of content generated freely by children themselves.

OHCHR notes that article 14 related to on-line child sexual abuse or material is currently formulated with insufficient precision.

Article 14(4) of the current draft provides that States 'may take steps to exclude the criminalization of children for self-generated material' and for material produced as part of a consensual sexual relationship. The element of 'taking steps' as well as the optional character of the provision weakens this exclusion and does not offer sufficient protection of the rights of the child as required by international law. As noted by the Committee on the Rights of the Child, '(s)elf-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized'.

OHCHR proposes the following text for article 14(4):

States Parties ~~may take steps to~~ ***shall*** *exclude the criminalization of States Parties shall exclude the criminalization of:*

(a) Conduct by children for self-generated material depicting them as described in paragraph 2 of this article; or

(b) Conduct set forth in paragraph 1 of this article, relating to material described in paragraph 2 (a) to (c) of this article, where such material is produced as part of a consensual sexual relationship, as determined by domestic law and consistent with applicable international obligations, and is maintained exclusively for the private and consensual use of the persons involved.

AN EXPLICIT EXCEPTION FOR ARTISTIC, EDUCATIONAL AND SCIENTIFIC MATERIAL IN RELATION TO THE TERM 'CHILD SEXUAL ABUSE MATERIAL'

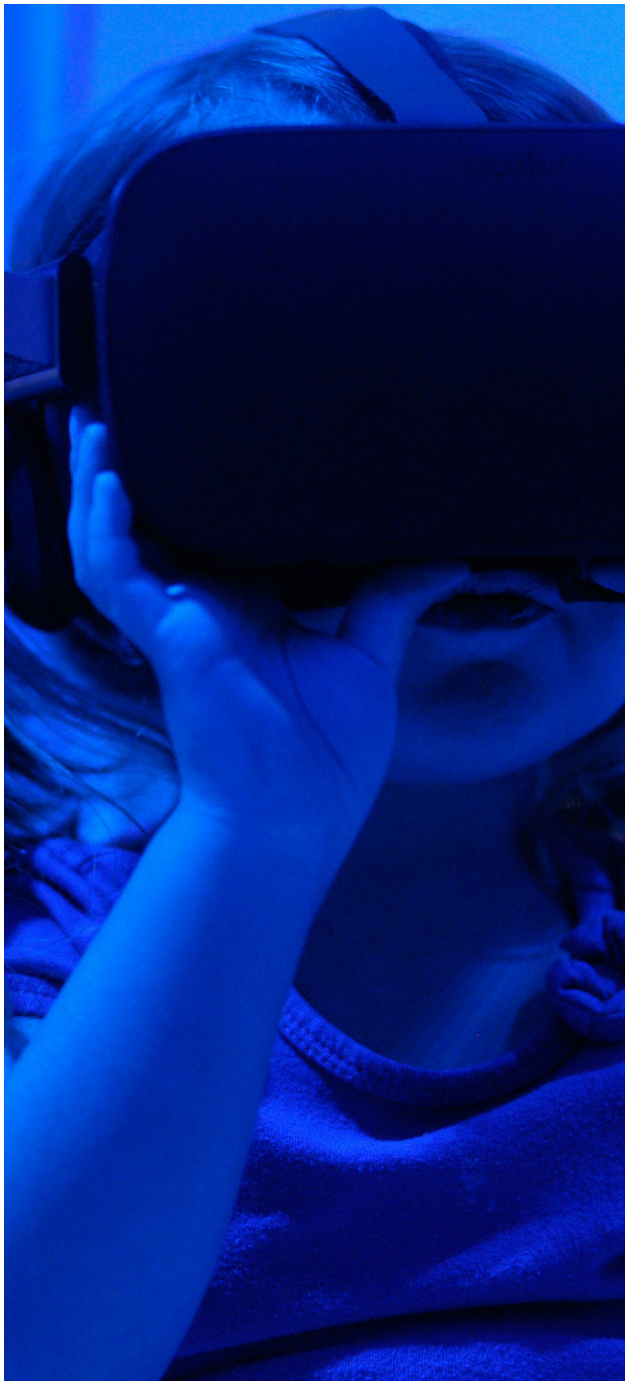
The criminalization of content that 'represents' a child in article 14(2) could cover, for example, legitimate expressions of art, literature and science depicting fictitious individuals, as well as news reporting or historic research about instances of child sexual abuse. It is important to avoid that the Convention could be used as a basis for improper censorship of material.

To clarify the type and scope of content considered to be 'child sexual abuse material', OHCHR recommends an explicit exception for artistic, educational and scientific material as a new article following article 14(2):

Material of manifestly artistic, educational, or scientific character and without the involvement of persons under the age of 18 years shall be exempted from art 14(1).

PROTECTION OF INDIVIDUALS UNDER 18

Article 16 currently requires the criminalization of the 'selling', 'distributing', 'transmitting', 'publishing', or 'otherwise making available' an intimate image of a person by means of an information and communication technology system without consent. However, the current version of article 16(2) restricts the criminalization requirement to the sharing of intimate images without the consent of individuals over the age of 18. While the reasoning behind this restriction appears to be that children cannot consent to sharing of intimate images, the current formulation might leave a protection gap for individuals below the age of 18, whose images are shared without their consent. Article 16(3) provides States the discretion to extend article 16 to children under the age of 18 if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.



Photos by Unsplash: Giu Vicente

OHCHR recommends the following amendment:

*A State Party ~~may~~ **shall** extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.*

LIABILITY OF LEGAL PERSONS

Article 18 would require from States Parties to establish liability of legal person "for participation in the offences in accordance with this Convention". The current draft does not require any intentionality whatsoever, in contrast to article 19 that includes such a condition. This would risk extending liability of service providers for any acts of their users, including any content uploaded or shared by them. This would force service providers to take the strictest measures possible to avoid liability, including the scanning of all communications and data on their services. It would thus require undue interferences with the right to privacy on a mass scale and incentivize the removal and blocking of vast arrays of human rights protected content. To avoid such outcomes, article 18(1) should be amended.

OHCHR recommends the following amendment:

Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention, ***if the legal person had at a minimum actual knowledge of the specific offence committed.***

PROCEDURAL MEASURES AND CONDITIONS AND SAFEGUARDS

The draft Convention requires the introduction of procedural measures for the purpose of facilitating criminal investigations and proceedings. Such measures relate to issues such as the search and seizure of data, the preservation of data and even the interception of content data.

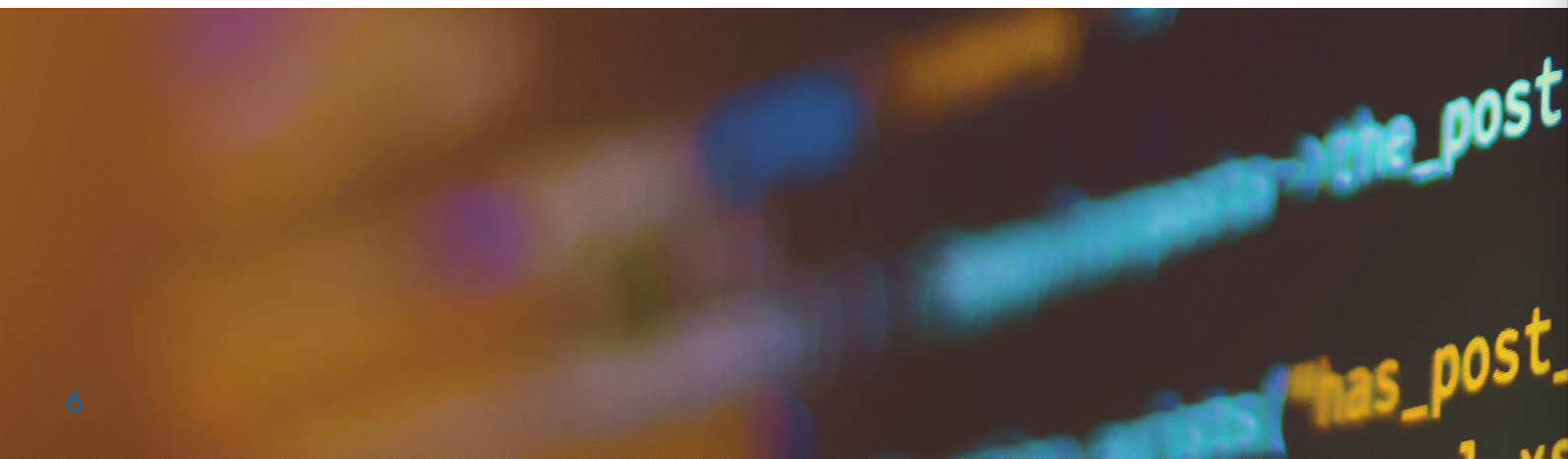
Several of the procedural measures relating to the investigation of cybercrime are intrusive in nature. These require stringent safeguards in response to prevent misuse of measures and possible abuse of human rights.

KEY MESSAGES

OHCHR recommends:

- The deletion of current article 28(4) (search and seizure of stored data)
- The deletion of current article 29 (real-time collection of traffic data) and article 30 (interception of content data).
- The restriction of the scope of current Chapter IV (procedural measures and law enforcement) to the criminal offences established in current Chapter II.
- The inclusion in article 23(1) of a requirement that any procedural measure in connection with the investigation of a specific criminal offence under the Convention is both necessary and proportional.
- The inclusion of a general clause on safeguards.

Photos by Unsplash: Markus Spiske



DELETION OF THE ARTICLE 28(4) 'SEARCH AND SEIZURE OF STORED DATA'

Article 28 sets out the requirements to empower competent authorities to search and access a computer system and its stored data. Article 28(4) requires measures that would allow competent authorities to order a person to provide information to enable these search and seizure measures.

This measure carries risks for the effective protection of human rights, notably the right to privacy.

For example, the provision could allow States to compel third parties to disclose vulnerabilities of certain software, in other words assist the State to find ways to enter a computer system. Similarly, it could allow the State to force a third party to assist it to access encrypted communications. Such third parties would not only include the operators of the ICT system at issue, but any person, including the operator's employees.

This could enable surveillance of various kinds of communications, leading to disproportionate interference with the confidentiality of communications. States could also alter the content of communications, interfering with freedom of expression and other rights.

International human rights law requires States to abstain from undue interference in the right to privacy and to take measures to ensure the necessary level of security, integrity and confidentiality of communications so that people can enjoy their privacy. If authorities were permitted to compel third parties as proposed in article 28(4), such access could be readily applied for a range of broader, unrelated purposes, such as surveillance, without a requirement of judicial authorization.

DELETION OF THE ARTICLES ON 'REAL-TIME COLLECTION OF TRAFFIC DATA' (ARTICLE 29) AND ON 'INTERCEPTION OF CONTENT DATA' (ARTICLE 30)

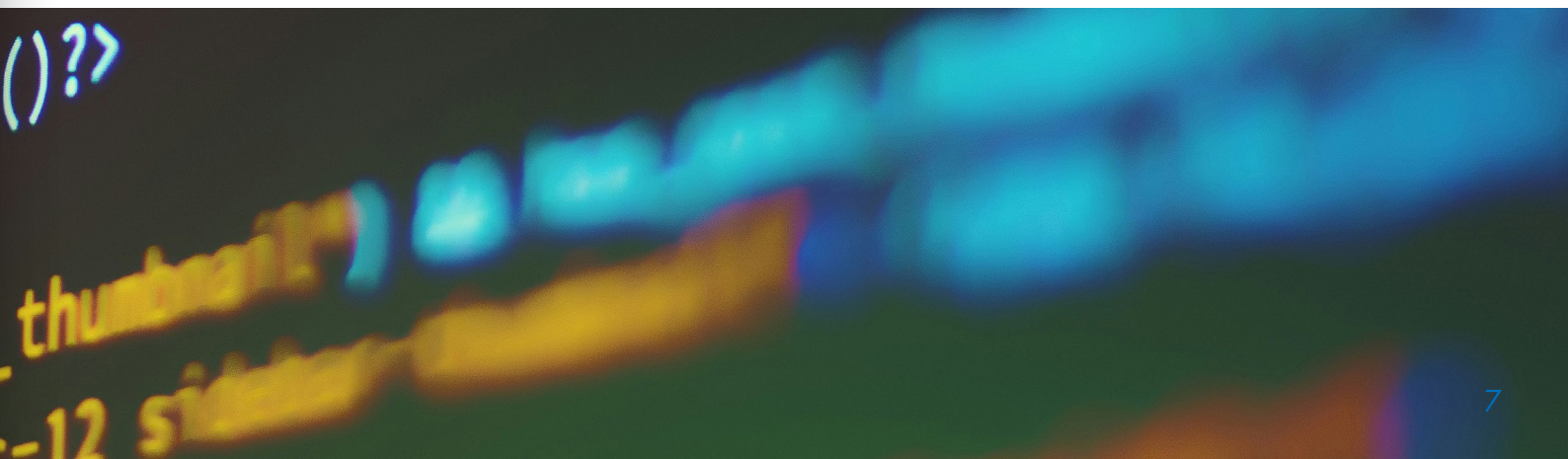
The 'real-time collection of traffic data' and the 'interception of content data' are very intrusive in nature and could result in massive data collection. Their use would be disproportionate in many cases, except possibly for the most serious crimes. Moreover, the article, as currently drafted, does not require judicial authorization for such intrusion.

Imposing an obligation under the Convention to conduct such measures for a broad range of criminal offences and without a clear requirement of prior judicial authorization to assess lawfulness, necessity and proportionality of the measures, would pose major risks of misuse and abuse through arbitrary interference with the right to privacy. Moreover, many States' legal frameworks and institutional capacities might not be prepared to prevent and mitigate these risks.

RESTRICTION OF THE SCOPE OF PROCEDURAL MEASURES IN CHAPTER IV

Article 23 expands the operation of the procedural measures in Chapter IV to cover not only criminal offences established in the Convention, but also other criminal offences committed by means of information and communications technology systems as well as the collection of evidence in electronic form of any criminal offence. This would expand the operation of the Convention beyond the criminal offences identified in Chapter II.

If it is nevertheless decided that the scope of procedural measures should be broader than the criminal offences established in the Convention, OHCHR recommends limiting the scope of procedural measures to 'serious crimes', defined



as a crime carrying a punishment of a maximum deprivation of liberty of at least four years applies in both the requesting and the requested State, and with an additional qualitative element of 'harmfulness' applied to the offence, such as death or bodily harm, clearly defined financial crimes or infliction of coercive acts.

Accordingly, the definition of 'serious crimes' currently in article 2 should be amended as follows:

'Serious crime' shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty ***in both the requesting and requested State and involving death or bodily harm, financial crimes or coercive acts****;*

Photos by Unsplash: Matthew Tenbruggencate

CONDITIONING OF PROCEDURAL MEASURES RELATED TO INVESTIGATIONS

Article 23 provides that all procedural measures, except for the interception of content data, could be available to investigate any sort of crime, whether established in the Convention or not, irrespective of the nature and gravity of the criminal offence in question.

For example, provisions of search and seizure of computers and data under the Convention might be activated for 'lèse majesté' crimes or for artistic expressions that might be considered 'propaganda against the State', when they are in fact legitimate expressions under human rights law.

In this regard, OHCHR recommends that article 23(2) limits the scope of procedural measures to criminal offences established under the Convention and to serious criminal offences as defined below.

OHCHR proposes the following revised version of article 23(2):

Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to.

1. The criminal offences established in accordance with this Convention;

2. Other criminal offences ***considered serious criminal offences*** *committed by means of an information and communications technology system; and,*

3. The collection of evidence in electronic form of any ~~criminal~~ offence ***established in accordance with this Convention or of serious criminal offences****.*

GENERAL CLAUSE ON SAFEGUARDS

There is a lack of explicit language to ensure:

- That there are reasonable grounds to believe that a criminal offence has been or will be committed and that relevant information concerning the offence would likely be obtained through the measure;

- That the procedural measures applied are subject to safeguards in line with States' obligations under international human rights law.

A failure to focus the operation of procedural measures in this way could mean that the Convention would enable States to initiate intrusive measures against individuals, which may give insight into an individual's behaviour, social relationships, private preferences and identity, without demonstrating a justified suspicion of a crime having been or being committed.

A general safeguards clause should apply to the operation of the entire Convention - not just the provisions on procedural measures - and include explicit references to:

- the principles of legality, necessity and proportionality

- prior judicial review of the exercise of procedural powers

- limitations of the scope and duration of procedural powers

- adequate notification and other transparency measures for affected individuals and entities

- access to effective remedies for anyone affected or otherwise suffering harm as a result of the exercise of procedural powers

- respect for the confidentiality of privileged communications, including attorney-client communications.

To this end, OHCHR recommends the following general clause on safeguards in Chapter 1, replacing article 24 in Chapter IV:

> *1. The obligation to establish, implement and apply any of the powers and procedures under this Convention applies only insofar as it is necessary for the investigation of specific criminal offences established by this Convention.*
>
> *2. States Parties shall ensure that such powers and procedures are carried out only if a factual basis gives reason to believe that a criminal offence established by the Convention has been or will be committed and that relevant information concerning the offence will be obtained through the measure.*
>
> *3. Those powers and procedures shall be subject to effective conditions and safeguards, in accordance with the State Party's obligations under international human rights law. Such conditions and safeguards shall, inter alia, incorporate the principles of legality, necessity and proportionality, require prior judicial or other independent authorization and review of the exercise of those powers, establish limitations of the scope and the duration of such powers or procedures, provide for adequate notification and other transparency measures for affected individuals and entities, provide for access to effective remedies for any individual suffering damage as a result of the exercise of such powers or procedures, and respect confidentiality of attorney-client and other privileged communications.*
>
> *4. Confidentiality of powers and procedures under this Convention, including when imposed on service providers, shall be limited to the time period and extent necessary to enable the effective investigation of the specific crime at issue. All persons affected by the powers and measures at issue shall be notified as soon as such notification may not interfere with the effective investigation of the specific crime.*

INTERNATIONAL COOPERATION AND MUTUAL LEGAL ASSISTANCE

The scope of criminalization referred to above has a direct impact on the extent of international cooperation and mutual legal assistance required under the Convention.

KEY MESSAGES

OHCHR recommends that the Convention should include a clear framework for international cooperation, ensuring that States can cooperate meaningfully and without overwhelming the capacities of requested States, while mitigating the risk of potential abuse of the enjoyment of human rights. To that end, OHCHR proposes:

- Restriction of provisions on international cooperation to criminal offences clearly established by the Convention itself
- If the convention expands the scope of international cooperation beyond only criminal offences clearly established by the Convention, then limitation of cooperation to only 'serious criminal offences'
- Adequate conditions and safeguards for international cooperation and legal assistance
- The inclusion of general and mandatory clauses for refusal of any forms of international cooperation and mutual legal assistance in specific circumstances.

SERIOUS CRIMINAL OFFENCES LIMITATION

Focusing international cooperation on a limited range of criminal offences – either to those set out in the convention or to clearly defined 'serious criminal offences' – would ensure a clearer framework.

While OHCHR prioritizes a restriction of international cooperation to crimes set out in the Convention, the alternative of restricting international cooperation to 'serious criminal offences', could at least be relatively specific if that term was sufficiently precisely defined.

If the Convention employs the term 'serious criminal offences', it should be defined with a requirement that the maximum deprivation of liberty of at least four years applies in both the requesting and the requested State, and with an additional qualitative element of 'harmfulness' applied to the offence, such as death or bodily harm, clearly defined financial crimes or infliction of coercive acts (see previous section on Procedural Measures).

CONDITIONS AND SAFEGUARDS FOR INTERNATIONAL COOPERATION AND LEGAL ASSISTANCE

It would be important to ensure that provisions on international cooperation and legal assistance are compatible with international human rights law and avoid a situation where a State might be requested to cooperate with another State in a way that might compromise its human rights obligations. An example would be where a State, in using criminal law to prosecute a political opponent for her legitimate use of her right to freedom of expression, seeks access to stored electronic data, such as emails or accounts, without giving an explanation to the requested State. The provisions on cross-border data sharing do not require independent oversight or other safeguards. Law enforcement authorities in the requested State might therefore hand over private data about this person, without the request being subject to independent oversight, and without the requesting State having to show that the data is necessary for the investigation of a specific criminal offence.

It is therefore essential that the Convention provides for conditions and safeguards with respect to international cooperation. Against this background, OHCHR welcomes the inclusion of article 23(4) that extends the application of article 24 to cooperation scenarios. However, the framework established this way still lack clarity and specificity. the proposal for a general safeguards clause, as provided above would ensure a stronger human rights protection framework.

EXAMPLE OF THE BASIS FOR REFUSAL OF MUTUAL LEGAL ASSISTANCE

In some cases, a State might have grounds, including based on its international human rights obligations, to refuse international cooperation or legal assistance. For example, a State has charged a journalist for posting an article on-line and seeks mutual legal assistance to access real-time traffic data. This could place the requested State in a position where it could be complicit in violating the human rights of the journalists if it complied with the request under the Convention. Consequently, the Cybercrime Convention should include at least the following three bases to refuse international cooperation and mutual legal assistance:

- Where there is an absence of dual criminality – in other words, where not all cooperating states have criminalized the act subject to international cooperation and mutual legal assistance

Photos by Unsplash: Tobias Tullius

- Where the request for international cooperation and legal assistance relates to political offences

- Where there is a reasonable belief that assistance could contribute to violations and abuses of human rights, including but not limited to discrimination prohibited under international human rights law.

Against this background, OHCHR welcomes the inclusion of article 40(22), which would cover prosecutions and punishments on the basis of prohibited grounds for discrimination. The ground for refusal should be expanded to cover human rights violations more broadly and be made mandatory as an expression of the duties to respect and to protect under international human rights law.

Proposed amendment to article 40:

21bis Mutual legal assistance shall be refused (a) if there are reasonable grounds to believe that the criminal offence will be treated as a political offence by the requesting State; (b) if there are reasonable grounds to believe that the cooperation or assistance will result in a violation of human rights; (c) if 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;

22. ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ Mutual legal assistance shall be refused 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.

SUMMARY OF TEXTUAL PROPOSALS

Title

United Nation Convention against Cybercrime ~~(Crimes Committed through the Use of an Information and Communications Technology System)~~

- **Article 2**

"Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty ***in both the requesting and requested State and involving death or bodily harm, financial crimes or coercive acts;***

- **Article 4**

Deletion of the article.

- **General provision on conditions and safeguards**

1. The obligation to establish, implement and apply any of the powers and procedures under this Convention applies only insofar as it is necessary for the investigation of specific criminal offences established by this Convention.

2. States Parties shall ensure that such powers and procedures are carried out only if a factual basis gives reason to believe that a criminal offence established by the Convention has been or will be committed and that relevant information concerning the offence will be obtained through the measure.

3. Those powers and procedures shall be subject to effective conditions and safeguards, in accordance with the State Party's obligations under international human rights law. Such conditions and safeguards shall, inter alia, incorporate the principles of legality, necessity and proportionality, require prior judicial or other independent authorization and review of the exercise of those powers, establish limitations of the scope and the duration of such powers or procedures, provide for adequate notification and other transparency measures for affected individuals and entities, provide for access to effective remedies for any individual suffering damage as a result of the exercise of such powers or procedures, and respect confidentiality of attorney-client and other privileged communications.

4. Confidentiality of powers and procedures under this Convention, including when imposed on service providers, shall be limited to the time period and extent necessary to enable the effective investigation of the specific crime at issue. All persons affected by the powers and measures at issue shall be notified as soon as such notification may not interfere with the effective investigation of the specific crime.

- **Article 7**

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed ~~intentionally~~ ***with dishonest or criminal intent****, the access to the whole or any part of an information and communications technology system without right.*

2. A State Party may require that the offence be committed by infringing security measures, ~~with the intent of obtaining electronic data or other dishonest or criminal intent~~ or in relation to an information and communications technology system that is connected to another information and communications technology system.

Similar changes should be made to articles 8-10 and 12.

- **New article following article 14(2)**

Material of manifestly artistic, educational, or scientific character and without the involvement of persons under the age of 18 years shall be exempted from art 13(1).

- **Article 14(4)**

*States Parties ~~may take steps to~~ **shall** exclude the criminalization of States Parties shall exclude the criminalization of:*

(a) Conduct by children for self-generated material depicting them as described in paragraph 2 of this article; or

(b) Conduct set forth in paragraph 1 of this article, relating to material described in paragraph 2 (a) to (c) of this article, where such material is produced as part of a consensual sexual relationship, as determined by domestic law and consistent with applicable international obligations, and is maintained exclusively for the private and consensual use of the persons involved.

- **Article 16(3)**

*A State Party ~~may~~ **shall** extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.*

- **Article 18**

*Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention, **if the legal person had at a minimum actual knowledge of the specific offence committed**.*

- **Article 23(2)**

Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to.

1. The criminal offences established in accordance with this Convention;

*2. Other criminal offences **considered serious criminal offences** committed by means of an information and communications technology system; and,*

*3. The collection of evidence in electronic form of any ~~criminal~~ offence **established in accordance with this Convention or of serious criminal offences**.*

- **Article 28(4)**

Deletion of the paragraph.

- **Articles 29 and 30**

Deletion of both articles.

- **Article 35(1)(c)**

The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, ~~including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention~~.

- **Article 40(21bis) & 22**

21bis Mutual legal assistance shall be refused (a) if there are reasonable grounds to believe that the criminal offence will be treated as a political offence by the requesting State; (b) if there are reasonable grounds to believe that the cooperation or assistance will result in a violation of human rights; (c) if 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;

22. ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ Mutual legal assistance shall be refused 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.

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Palais des Nations,
CH-1211 Geneva 10, Switzerland
www.ohchr.org