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

Sixth Session

21 August – 1 September 2023

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

22 August 2023

I. Introduction

The Office of the United Nations High Commissioner for Human Rights (OHCHR) welcomes the publication of the zero draft in June 2023 of the future UN cybercrime Convention.

OHCHR is pleased to observe that the zero draft incorporates several points and suggestions that were brought forward by Member States, civil society organizations, other stakeholders and OHCHR itself to ensure that the new Convention will uphold human rights. The zero draft provides a strong basis for further discussion, and we encourage the Ad Hoc Committee's continued openness in the process and the involvement of multi-stakeholder participation on an issue which is cross-sectoral and which has direct implications for society, people and individual rights.

At this stage, we would like to offer our comments first of all on some key positive developments in the zero-draft compared to the consolidated negotiating document (CND). We strongly suggest these developments to be retained, and only strengthened as the negotiations progress. Secondly, we offer comments on some of the critical points arising from the zero draft that we believe would require further attention and amendment. Our comments are not intended to be exhaustive nor to offer a detailed analysis of each article. As in previous submissions, our comments contain observations on human rights considerations arising from the review of the zero draft, 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.

II. Key positive developments

Narrower scope of criminalization

OHCHR welcomes the zero draft's narrower approach to criminalization in Chapter II. OHCHR has in earlier submissions[1] advocated for a narrow scope of the future convention that should focus primarily on cyber-dependent crimes, and cautioned against including a wide range of cyber-enabled criminal offences and of acts whose criminalization would be incompatible with international human rights law. We welcome the exclusion of some of these offences from the zero draft, particularly the exclusion of speech-related offences found earlier in the CND cluster 8 and 9. We moreover welcome the attempts to bring the existing criminal offences described in chapter II into line with the principle of legality, by providing more precise descriptions of the acts sought criminalized. We will in the subsequent sections provide recommendations for how to strengthen this further.

Deletion of some intrusive measures

We welcome that article 87 of the CND which introduced "special investigative techniques" has not been retained in the zero draft.[2] Similarly, we are pleased to note that the provision on direct cross-border request to service providers is not included in the zero draft and that there is no direct obligation for States to cooperate in intercepting content of communication. We strongly advice against the reintroduction of these measures.

III. Critical points

The scope of the convention as currently set out in the zero draft is complex and involves different scopes relating to criminalization, law enforcement/procedural measures, technical cooperation, mutual legal assistance and safeguards. The interplay of the various scopes would benefit from further precision and clarification, particularly the relationship and interplay between articles 3, 17, 21, 35 and 40. For example, we recommend that the draft clarify in specific terms that the safeguards included in the chapter on law enforcement and procedural measures apply equally to international cooperation and legal assistance.

The following section provides selected comments on what OHCHR believes are key issues. The comments should be read in conjunction with language suggestions included in the zero draft itself, annexed to this comment.

[1] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf and https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf.

[2] See concerns raised about this provision in https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/OHCHR_submission_5th_session_Ad_Hoc_Committee_Cybercrime.pdf.

Preamble and Chapter I (General Provisions)

In the preamble, we welcome references to the right to privacy and human rights. With respect to subsection 12 of the preamble, we believe it is important to enhance the language and accurately reflect the language of international human rights law when it comes to the right to privacy. We suggest the following language: "*Stressing the right to protection against unlawful and arbitrary interference with the right to privacy, including the protection of personal data".* Given that many of the articles of the convention, both in the chapter on criminalization and in the chapters on law enforcement and procedural measures, have an impact on the right to freedom of expression, we recommend recognizing also this right explicitly in the preamble.

We are pleased to see that article 2(h) includes a quantitative threshold for "serious crimes". However, an additional threshold would be preferable to avoid arbitrary application, as in many jurisdictions the four year threshold would encompass a wide range of criminal offences, including offences which are not serious in nature. We therefore recommend, in line with earlier comments, to add a qualitative threshold, such as "and causing death or serious bodily harm" to complement the quantitative threshold.[3]

We welcome that article 5 underscores respect for human rights but note that it is a bare minimum human rights clause which excludes important aspects that were discussed during the negotiations and which featured in the CND. We strongly recommend the reintroduction of those elements either in article 5, or as a minimum, in the preamble. In view of the range of rights particularly impacted by the implementation of the convention, we believe it would be important to include explicit reference to specific international human rights instruments, in particular the International Covenant on Civil and Political Rights, as well as to the principles of legality, necessity, proportionality, transparency, oversight and access to remedies.[4] Finally, we note that the current version would not fully address situations where the Convention could impose obligations on States parties that would conflict with their obligations set out in international human rights law. OHCHR recommends adding a clarification that in such cases human rights obligations would prevail. For example, the following sentence could be added at the beginning of article 5: *"Nothing in the present convention should be interpreted as impairing any obligations of the States Parties under international human rights law."*

Chapter II (Criminalization)

Qualified intent as default

We note that the zero draft would still enable the criminalization of legitimate acts, done without any criminal intent or causing any harm. For example, article 6 could allow the

[3] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/OHCHR_submission_5th_session_Ad_Hoc_Committee_Cybercrime.pdf. As noted in that submission, "serious crime" is not defined under international law. 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).

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

imposition of criminal penalties on independent cyber security researchers. This raises the risk of chilling crucial cybersecurity work, with potentially highly detrimental effects on the cybersecurity of all. The carve-out in article 10(2) would not help in this regard, as it only applies to article 10 itself and requires that the testing had taken place with authorization.

One way to address the problem of the possible criminalization of legitimate, and societally even beneficial acts, would be to add a qualification to the intent requirements, such as for example "criminal intent", "dishonest intent" or the like. Criminal intent, or other appropriately defined forms of qualified intent, should be a default requirement for articles 6-12, and not discretionary, as it is currently with respect to some of the provisions (see for example, article 7(2); article 11(2)).

Conditions for criminalization

As mentioned above, we welcome the overall narrower approach to cybercrime in the zero draft compared to the CND. Notwithstanding, several of the criminal offences set out in chapter II require further precision in order to comply with the principle of legality as a central element of the rule of law. The principle of legality requires a criminal offence to be clearly defined in the law so that on the one hand individuals can have a clear understanding of what conduct is prohibited and what the consequences of such conduct will be in order to be able to comply with the law, and on the other hand to prevent arbitrary application of criminal law.

Articles under chapter II that require further precision:

Article 13: As highlighted in earlier submissions, combatting and preventing child sexual abuse and exploitation is a matter of utmost importance. We emphasize the importance of placing the rights of children and their best interest at the center when crafting these articles.

One matter of concern in the current draft remains that it does not sufficiently address the possibility that its wording could enable the criminalization of children themselves. While article 13(4) is significantly improved compared to the CND, the language would still expose children to criminalization for sexual activities. We recommend deleting from article 13(4) the words "*take steps to*", as this is a weak requirement that falls short of obligations under the Convention on the Rights of the Child to exclude the criminalization of children.[5] We furthermore highlight that the limitation of article 13(4) to "*self-generated*" material does not protect partners that consensually possess material, which is something that is protected under the Convention on the Rights of the Child.[6]

In line with the Convention on the Rights of the Child, we also suggest the following addition at the end of article 13(5): "*States Parties should make every effort to create and use alternatives to a criminal justice response*".[7]

[5] Committee on the Rights of the Child, General Comment 25, para 118; Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/156, para 67.
[6] Ibid.
[7] Committee on the Rights of the Child, General Comment 25, para 117.

We furthermore note that several of the acts in article 13(1): "broadcasting", "displaying", "publishing", "soliciting", "accessing or otherwise engaging with", "facilitating", are not included in the corresponding article in the Budapest Convention, nor in the Convention on the Rights of the Child, Second Optional Protocol.

OHCHR is further concerned that article 13(2) may be phrased in a way that could unduly criminalize some forms of artistic expression and scientific research. In particular, the inclusion of "written material" in article 13(2) could cover many works of literature and science that describe or refer to sexual acts involving minors or other children. Often, these references are made to describe historical events or provide commentary on social developments and the current version of the provision would risk outlawing such material. OHCHR recommends therefore not to include written materials among the material covered by article 13.

Article 14: We note that this article appears to be overly broad. Firstly, it would cover communication with children who are above the minimum age of consent. Secondly, the term "sexual purposes" lacks any definition and could be interpreted and implemented in overly broad ways, effectively outlawing protected activities and expression.

Article 15: The protection against the non-consensual dissemination of intimidate images, often extremely harmful to the persons affected, is an important issue. However, we believe that the current version does not succeed in addressing the complex issues relating to how to regulate such acts.

The definition of "intimate images" contains vague elements that make the provision susceptible to overreach. The term "sexual activity" used to define "intimate image" could be understood in many ways, depending on region, traditions and legal system. Without further clarifications, it could include many aspects and actions of inter-personal life, such as kissing or holding hands. The term could also be misinterpreted and applied in a way that would discriminate same-sex interactions, often targeted under unduly extensive obscenity and pornography laws.

Furthermore, it is unclear what the draft definition is covering by referring to a "representation of a natural person". The juxtaposition with the term "visual recording" seems to suggest that all kinds of possible other forms of depicting a person could be covered, including drawings or caricatures. While such depictions can indeed be hurtful to the persons represented, it is doubtful that all such representations would be as harmful as real recordings and should be subject to criminalization.

Moreover, there are circumstances where it can be justifiable to share images covered by the draft provision. For example, a photograph proving an affair of a politician could be in the public interest to be accessible. An intimate image could also be important evidence identifying the perpetrator of a sexual assault that is being discussed by the public and could thus be published for good reason. The current draft should at least contain exceptions for these kinds of scenarios.

Finally, there are areas that deserve further discussion to ensure that any obligation with regard to intimate images resulting from the Convention would be properly targeted.

These include possible harm requirements and their scope; related intent requirements; and the necessity of the identifiability of the depicted person.

Article 17 appears to broaden the scope of the convention to include all criminal offences as covered by other international conventions and protocols. On its own, article 17 appears redundant, as it requires States to ensure that "offline" offences under other international conventions and protocols are also criminalized if they are committed through the use of a computer. Such situations would generally already be covered by each respective convention.

A central question is how article 17 relates to articles 35 and 40, and if all crimes that fall under article 17 automatically are considered "serious crimes" for the purpose of the convention as a result of the formulations in article 35 and 40 (*"(...) as well as of serious crime, including those offences covered by article 17 of this Convention when applicable"*). Such a result would contradict the efforts in other parts of the Convention to clearly describe and limit the scope of application of the Convention and its Chapters.

Similarly, the inclusion of article 17 also appears to affect the meaning of the many references to *"offences covered by this Convention"*. If understood as also including all offences to be criminalized under article 17, the careful delineations of scopes of application across the Convention would become moot. For example, cooperation measures seemingly limited by article 35 could become applicable to a far broader range of offences that are neither criminalized under articles 6-16 nor serious.

In view of its unclear purpose and lack of clarity, OHCHR recommends the deletion of article 17.

Article 19(3): This provision allows for the criminalization of preparation of an offence under articles 6-16. OHCHR would like to note that the criminalization of acts below the threshold of "attempt" (already covered under article 19(2)), should be limited to acts that are so inherently dangerous that such wide-reaching criminalization is necessary. Thus, we recommend its deletion.

Article 20: The statute of limitations provision in article 20 requires States Parties to establish a longer statute of limitations for criminal offences established under articles 6-16 of the Convention but does not establish a maximum time limit. The provision further allows for suspension of the statute of limitations altogether in situations where the alleged offender has evaded the administration of justice. While the provision provides that the gravity of the criminal offence should be considered before extending the statute of limitations, we are concerned that such a provision fails to meet the requirement of proportionality. At a minimum, we believe that extension of the statute of limitations should be left at States Parties' discretion and not made mandatory (as it currently is through the word "shall"). We would furthermore like to note that by comparison, the corresponding article under UNTOC does not allow for a suspension of the statute of limitations but instead allows State to establish "a longer period" of statute of limitations situations where the alleged offender has evaded the administration of justice.[8]

[8] UNTOC article 11(5): "Each State Party shall, where appropriate, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence covered by this Convention and a longer period where the alleged offender has evaded the administration of justice."

Chapter III (Jurisdiction)

Article 22: We would like to note that article 22(1) (d) appears overly broad, as the reference to "*State Party*" could be interpreted to cover all kinds of State institutions, infrastructure, officials etc. In view of the other elements of jurisdiction covered under article 22 (1) and (2) we suggest deletion of article 20(1) (d).

Chapter IV (Procedural Measures and Law Enforcement)

Article 23 establishes the scope of procedural measures. The scope defined by article 23(1) and (2) are in our view broader than what is necessary for the purposes of the convention to establish a baseline for international cooperation and coordination. Article 23 in its current version does not consider a central concept in criminal law and procedure whereby the initiation of procedural measures requires a minimum element of fact-based reasonable grounds that a criminal offence has been committed or is being committed. Without a justified suspicion of a crime having been or being committed, it would not be necessary to initiate procedural measures for achieving a legitimate goal. Therefore, the absence of a requirement of reasonable grounds to believe that a measure is necessary to support investigating and solving a specific crime represents a gap that risks running afoul of human rights requirements.[9] This is particularly problematic given that the specific measures defined by articles 25 et seqq generally fail to establish any concrete meaningful definition of thresholds and conditions that are proportionate to the intrusiveness of the measures at hand.

Under the zero draft, all of the law enforcement and procedural measures, except for the interception of content data, could apparently be available to investigate any sort of crime, irrespective of the nature and gravity of the criminal offence in question. This would be irreconcilable with the principle of proportionality, even if the possibility to make reservations with regard to some of the measures exist. Of particular concern in this connection is article 29, given that access to traffic data (whose definition in the zero draft is very broad, and indeed broader than what is found in the Budapest Convention) can give an extremely detailed "insight into an individual's behavior, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication".[10]

Article 23 opens thus up for procedural measures to be applied irrespective of a link to the investigation of a specific crime. We recommend further strengthening this provision to ensure that the scope of procedural measures is connected to the reason for which they are needed. In article 23(1) we recommend adding at the end of the sentence the following addition: "*where there are reasonable grounds to believe that a criminal offence is committed or being committed*". This would ensure that procedural measures under the

[9] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf and https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf.

[10] Reports of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, para 19 and A/HRC/39/29, para 6.

convention are employed exclusively in connection with specific and targeted criminal investigations or proceedings. Such amendment is important since none of the individual provisions on procedural measures in Chapter IV have expressly established safeguards or conditions, including any language that would condition the procedural and law enforcement measures to the investigation of a specific criminal offence and where there are reasonable grounds to believe that such a criminal offence is committed or being committed. As an alternative, the individual provisions on procedural measures could include specific language establishing such a threshold for their application, similar to articles 45(1), 46(1) and 47(1) of the CND.

Article 23(2) gives reason for further concern. Letters (b) and (c) significantly expand the scope of crimes, to which procedural measures would apply, beyond the offences to be criminalized under the Convention. Both letters could permit procedural measures under Chapter IV to be applied with regard to effectively any criminal offence that leave a digital trail, which would amount to most criminal offences today. In other words, it allows for intrusive measures such as for example real-time collection of traffic data, even for minor criminal offences. Such an approach would be overly sweeping and raises compatibility issues with necessity and proportionality requirements under international human rights law. It would also considerably go beyond what is necessary for the purpose of this convention to establish a baseline for international cooperation.

To address this issue, we recommend a reconsideration of the language to ensure a proportional application of law enforcement and procedural measures. First, we recommend limiting the scope of procedural measures in article 23(2)(b) to "serious" criminal offences. Second, letter (c) could be dropped or at least limited to "serious crimes" as well.

Article 24: Article 24 on conditions and safeguards is a central article. We welcome its reference to international human rights law and the principle of proportionality but remain concerned that it is insufficient for offering adequate protection in view of the type of measures allowed on the basis of the convention. We note that the current language in article 24 is weaker than that found in the CND as well as that of the Budapest Convention. More generally, in our view article 24 despite its references to human rights law and some safeguards and conditions, is not sufficient in providing an adequate level of protections for individuals subject to or affected by procedural measures.

We recommend to further enhance article 24(1) through amending the language so it reads: "*Each 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 provide for the adequate protection of human rights consistent with its obligations under international human rights law, and which shall incorporate the principles of legality, necessity, and proportionality and necessitate a factual basis justifying access or application of such powers and procedures"* (added language underlined).

While article 24(2) contains important clarifications as to what conditions and safeguards States Parties would have to consider, we are concerned about several missing elements and a lack of specificity. Article 24(2) does not mention transparency and accountability measures, reflecting an overall lack in the zero draft to guarantee a sufficient level of transparency and accountability for procedural measures. While we recognize that

criminal investigations require a certain level of confidentiality in order to be effective, the typical secrecy only emphasizes the need for adequate oversight. Moreover, secrecy can only be justified to the extent that it is necessary to ensure that investigations are not put in peril. Once such a risk is not realistic anymore, the targets of the procedural measures should be notified. Without such notifications, individuals would face unjustifiable barriers to challenging intrusive measures -that may arbitrarily interfere with certain human rights-, which would undermine their ability to exercise their right to remedy. Moreover, other transparency measures, such as the publication of data about procedural measures taken, would enable accountability to the public. On this basis, we recommend adding transparency and access to remedies to article 24(2) and expressly narrowing secrecy requirements as provided in article 25(3), 29(3) and 30(3).

We are also concerned that the zero draft does not acknowledge the importance of, let alone take any steps to protect the confidentiality of attorney-client communications[11], doctor-patient communications and other forms of privileged communication, despite the obligations to do so under international human rights law. We recommend that such protection is explicitly included in the convention.

In addition, to bring article 24(2) in line with recognized standards for criminal investigations under international human rights law, we also recommend amendments to article 24(2) to ensure explicit reference to prior judicial/independent authorization and to link the scope and duration of measures to what is necessary and proportionate for the investigation of a specific criminal offence.[12]

In light of the foregoing and based on the current language of article 24(2), we suggest the following language: "*Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include prior judicial or other independent authorization and review, grounds justifying application, limitation of the scope and the duration of such powers or procedure to what is necessary and proportionate for the investigation of a specific criminal offence, adequate notification and other transparency measures, access to effective remedies, and confidentiality for attorney-client and other privileged communications."* (added language underlined).

Alternative language that would ensure a higher level of human rights protection but would deviate more from the current version of article 24(2) could be the following: "*Each 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 that ensure full respect of human rights in view of the nature of the procedure or power concerned, including judicial or other independent supervision, prior judicial or other independent approval, grounds justifying application and limitation of the scope and the duration of such power or procedure, adequate notification and other*

[11] See Basic Principles on the Role of Lawyers, adopted on 7 September by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, principle 22, according to which "Governments shall recognize and respect that all communications and consultations between lawyers and their clients within their professional relationship are confidential.". For further discussion of protection of confidentiality in the attorney-client relationship see the Report of the Special Rapporteur on the independence of judges and lawyers, A/71/348, paras 45-49.

[12] See Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/39/29, paras 37, 39-40.

transparency measures, access to effective remedies, and confidentiality for attorney-client and other privileged communications".

Article 24(3) on public interest appears to establish a problematic relationship between public interest and individual rights. The underlying rationale for public interest is not that rights should only be upheld to the extent that they are consistent with the public interest. Rather, the impact on people's rights must be fully taken into account, and restrictions are only acceptable in the public interest if they are necessary and proportionate. We recommend amending the provision so it reads: "*Each State Party shall consider the impact of the powers and procedures in this article that are taken in the public interest and for the proper course of justice upon the rights of individuals."*

Article 25: We recommend adding language in the provision that clarifies that the preservation order does not go beyond what service providers collect as part of what they offer in their products/services. We furthermore note that article 25(3) provides for confidentiality without specific limits or a criterion to establish it. We underline that confidentiality must have limits and there should also be a guarantee for transparency and access to remedy. We suggest adding language to enhance that confidentiality should be lifted when it is no longer prejudicial to an ongoing investigation.

Articles 26 and 27 currently use language that appears to allow the compelling of the retention of data of *all* users, including those not suspected of any criminal offence. Any surveillance measure must target specific individuals. We recommend adding this precision in articles 26 and 27, emphasizing that the measures are taken "*in relation to specified persons"*. While these articles appear similar to corresponding articles in the Budapest Convention, those articles make explicit reference to the provisions on safeguards and scope. We recommend including similar references in article 26 and 27, by adding the language "*subject to articles 23 and 24"* at the end of each article.

Article 28 raises a number of concerns. As noted in our earlier submission, personal electronic devices frequently contain highly sensitive personal information not only about their user/owner but also many third parties. Search and seizure measures for such devices therefore can carry greater risk to human rights, including the right to privacy, than covert access to data on a particular individual. It is essential that the convention recognizes the need for additional robust safeguards for search and seizure of personal devices and ensures that these measures are subject to sufficient independent oversight and control. Article 28(4) contains broad language, which goes beyond the corresponding article in the Budapest Convention, and which can be interpreted as compelling decryption or force disclosure of encryption keys, enable decryption orders and provide active assistance in decryption, and enable surveillance of various kinds. We recommend the deletion of article 28(4).

Article 29 concerning real-time collection of traffic data raises a number of concerns. First, given that real-time collection of traffic data is a highly intrusive act, it only should be possible for very serious offences, as otherwise it would likely be a disproportionate measure. Moreover, we recommend to add to article 29(1) a requirement of prior judicial authorization. Secondly, we note that article 29(3) amounts to a gag order without any time limits. We recommend adding to the end of article 29(3) the following addition: "*and only to the extent that such confidentiality is needed in order not to put the investigation at peril".* Furthermore, as with articles 27 and 28, and as found in the corresponding

article in the Budapest Convention, we recommend adding a sub-paragraph 4 to article 29, stating that "*The powers and procedures referred to in this article shall be subject to articles 23 and 24".*

Similar to article 29, **article 30** on interception of content data is a highly intrusive surveillance measure that should be approached with utmost caution. Indeed, imposing an obligation under the Convention to conduct such measures would pose immense risks for human rights, such as the right to privacy, in particular given the inadequacy of various domestic legal frameworks and institutional capacities to prevent and mitigate such risks. Against this background, we strongly recommend to the negotiating parties to re-consider the inclusion of real-time interception of content data.

Should article 30 remain in the Convention, it would be paramount to reflect the following considerations in its text. The interception of content data can only be justified as far as they are strictly necessary for achieving a legitimate aim and meet the proportionality requirement. It can only be justified for investigating or preventing particularly grave offences. The duration must be limited to the strict minimum necessary for achieving the specified goal, with rigorous rules on storing and using the data obtained. The initiation of such measures would need to rest on specific safeguards[13]; the interception of content data should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated. Those who have been the subject of surveillance should be notified and have explained to them ex post facto the interference with their right to privacy.

Article 31(8) contains unclear language and risks enabling an arbitrary and overly broad application. The paragraph appears to shift the burden of proof to the offender rather than the prosecution. This could be understood as affecting the right to be presumed innocent. At the same time, it refers to "offender" rather than to an "alleged offender" as other provisions of the zero draft, which raises the question if it only applies to cases where the offender has already been convicted. Even if so, it would not be clear whether the provision is limited to the execution of the conviction or would cover other legal proceedings as well. We suggest the deletion of this provision.

Chapter V (International Cooperation)

We welcome that **article 35** attempts to limit the scope of Chapter V measures rather than requiring cooperation measures, including measures that can deeply affect human rights, for all kinds of crimes. However, as explained above, the current definition of "serious crimes" still raises concerns, as it could easily encompass offences that are far from being serious. In addition to the changes to that definition that were discussed above, we also recommend strengthening the approach of the Convention to dual criminality. Firstly, we suggest amending article 35(2) so it firmly establishes dual criminality as a requirement. Secondly, in cases where the obligation to cooperate rests on the classification of the crime as serious, it should be required that it meets the conditions for seriousness in both the requesting and the responding state.

[13] See Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/39/29, paras. 34-41.

We note with regret that the reference that the CND's international cooperation Chapter previously made to the conditions and safeguards provision has been deleted from the zero draft. As a result, it is not clear from the structure of the zero draft that the conditions and safeguards for procedural measures as provided in article 24 also apply to measures of under Chapter V. This leaves Chapter V void of specific references to key safeguards that need to be in place for intrusive measures to be human rights compliant. We strongly suggest inserting explicit reference in article 35(1) to articles 23 and 24.

We furthermore note that article 35(1) refers to article 17 whose interpretation is unclear. It could be read in a way that offences covered by article 17 would have to be serious crimes in order to trigger international cooperation obligations under Chapter V. However, article 17 and article 35 as currently drafted, could possibly facilitate interpretations, according to which all kinds of criminal offences covered by article 17 could fall within the scope of Chapter V. This would lead to an extremely expansive and problematic application of international cooperation measures.

Article 36 contains positive elements which would enable States with data protection guarantees to maintain their standards and avoid sharing data in situations where the recipient will not be able to protect such data. However, we believe that the article's lack of reference to minimum requirements for data protection constitutes a weakness which could be rectified by adding specific reference to some of the minimum requirements for data protection: *the principles of lawful and fair processing, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability*. The Human Rights Committee has recognized data protection principles deriving from the International Covenant on Civil and Political Rights.[14] Similarly, the UN General Assembly and the Human Rights Council have recommended the adoption of data protection legislation in accordance with international human rights law.[15]

Article 37: We believe the grounds for refusal of assistance should be improved and enhanced. This includes broadening the language to expressly include as grounds for refusal the risk that assistance will represent a real and foreseeable risk of irreparable harm, and the risk that the request concerns an offence considered a political offence, or an offence connected with a political offence.

We also note that article 37(15) fails to incorporate all prohibited grounds of discrimination as a basis to refuse extradition. We recommend expanding the scope of article 37(15), by aligning it with the full scope of non-discrimination obligations under international human rights treaties.

Moreover, we note that article 37(9) allows for simplified evidentiary requirements, without the rationale for this being clear. We suggest the deletion of this provision.

Article 40: Article 40(4) contains language "*without prejudice to domestic law"* which could possibly be misread as allowing violation of domestic law for the purpose of information gathering/data collection for voluntary transmission to another State. We

[14] Human Rights Committee, General Comment No 16, para 21. See also Report of the United Nations High Commissioner for Human Rights, The Rights to Privacy in the Digital Age, A/HRC/39/29.
[15] See for example, A/RES/77/211, para 7(i).

recommend amending this provision, so it reads "*Subject to the provisions and procedures of domestic law, and in line with international human rights standards, the competent authorities ....”* We furthermore note that article 40(8) requires further revision to preclude assistance in the absence of dual criminality. In this connection we recommend replacing the word "may" with "shall" in the first sentence. Moreover, we recommend the deletion of the second sentence.

Article 40(21) is a key provision which ensures that States would not have to comply with demands that would go against international human rights law. We believe that this provision can be further strengthened by making clear references to human rights and political offences, as the listed grounds in article 40(21)(b) would not necessarily cover all concerns. We recommend the following revisions: "*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; the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, or ordre public.”*

Please note in this context, that in Article 40(21)(c) we recommend replacing the words "be prohibited" with "not be authorized", so as to capture situations where there may not be an express prohibition but it is clear from the legal system that express authorization is needed, such as for example for surveillance of real-time communication.

Article 40(30)(b) allows for sharing of documents and information, but does not include any guarantee of privacy and data protection. We recommend adding at the end of the sentence the following conditions: "*subject to the right to privacy and data protection principles”.*

Article 41: We note that the scope of the proposed 24/7 network is very broad, covering different stages of the legal process and a range of offences. Such a broad scope could allow for data to be collected, stored and shared across borders, bypassing the processes for mutual legal assistance and the respective conditions and safeguards as provided in articles 24 and 36. We recommend narrowing the scope of this provision to focus on providing technical assistance during the initial stages of investigation of specific criminal investigations, and clarifying that the point of contact is not responsible for the collection, preservation or sharing of evidence. Moreover, we note that cross-border cooperation can lead to new privacy and information security risks, for example where requests are fraudulent or not authenticated or where information is provided over an insecure channel that enables interception by unauthorized parties. For this reason, we recommend adding requirements that channels for information exchange be secure, encrypted and include authentication mechanisms for requests and responses.

Article 47 mandates broad and open-ended law enforcement cooperation without sufficient safeguards as required under international human rights law. Article 47(1)(b), (c) and (f) allows States to share a broad range of information, including personal, data that would enable States Parties to circumvent safeguards in the framework of mutual legal assistance. We recommend deleting these provisions.

Chapter VI (Preventive Measures)

Article 53: Holistic and appropriate preventive measures are core to a successful criminal justice strategy. Well-planned and effective preventive measures not only prevent crime and victimization, but also contribute to sustainable development. We therefore welcome the zero draft's attention to preventive measures and the various elements that have been included in article 53. With respect to article 53(3) (g) we believe the language can be strengthened, in line with the Convention on the Rights of the Child, to first of all highlight children as rights-holders, and not solely as persons who need protection. Secondly, with respect to the reference to "revising" legal frameworks, we believe that this may be interpreted to impose a strict obligation to introduce legislation to achieve certain outcomes that involves blocking and remove legitimate expression. We recommend the following revision: "*Undertaking specific and tailored efforts to protect the rights of children online, including through education and training on and raising public awareness of child sexual abuse or child sexual exploitation online, as well as making efforts to guarantee the immediate removal of child sexual abuse and exploitation material;"*.

Chapter VII (Technical Assistance and Information Exchange)

Article 54: We recommend that article 54 add a requirement that any technical assistance and capacity building is conditional upon prior human rights impact assessment. In view of the existing examples of States providing support to other States to develop for example surveillance capabilities, we note that such form of capacity building often ignores the situation in the recipient State and the risk of the capacity being used at odds with States' obligations under international human rights law.[16]

Chapter VIII (Mechanism of Implementation)

OHCHR believes that a successful implementation of the Convention would rely on including human rights considerations both in the content of what is being assessed as well as through the process. First, the mechanism of implementation should assess the human rights implications of States' implementation of the Convention. Second, the process by which implementation is assessed should be inclusive and participatory, including through the involvement of civil society and human rights mechanisms. As highlighted in our earlier comments, we believe the convention should lay the foundation for ensuring that future implementation discussions will benefit from robust multistakeholder engagement.[17] To ensure this, we recommend clarifying Article 57(3), first sentence in the following way: *"The Conference of the States Parties shall adopt rules of procedure and rules governing the activities set forth in this article, including rules concerning the ~~admission and~~ meaningful participation of ~~observers~~ multi-stakeholders and civil society organizations, and the payment of expenses incurred in*

[16] See Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/51/17, para 56.

[17] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/OHCHR_submission_5th_session_Ad_Hoc_Committee_Cybercrime.pdf.

carrying out those activities." Moreover, in Article 57(6), the words "duly accredited in accordance with procedures to be decided upon by the Conference, may" should be replaced with "shall".

For further comments and language proposals, including concerning provisions not covered in this document, see the Annex to this submission.