ARTICLE 19's Comments on the "Zero Draft" of the UN Cybercrime Convention

Ahead of the sixth session of the Ad Hoc Committee drafting the international convention on cybercrime to commence on 21 August 2023 in New York, ARTICLE 19 raises its concerns about the latest draft of the Convention (Zero Draft). While several problematic substantive provisions have been removed from the earlier draft versions, we are concerned about the lack of consensus on the scope of offences covered by the law enforcement and data sharing provisions of the Convention. At the same time, human rights and due process safeguards do not apply to the bulk of these new powers. We also note that where safeguards are mentioned in the draft, they are at best limited and optional. This is coupled with numerous provisions encouraging general data sharing outside law enforcement proceedings under the Convention, and a failure to define what is meant by "data" and "information" in multiple instances.

ARTICLE 19 believes that this dangerous asymmetry in the Zero Draft opens the door to, and endorses, opening the floodgates of data sharing. This will give rise to significant abuse by States that already harness user data for surveillance and repression, utilizing rapidly evolving technologies such as biometrics and artificial intelligence. We urge the Ad Hoc Committee to seriously reconsider its efforts and make sure the draft provisions do not violate international human rights standards which the instrument explicitly requires adherence to and claims to prioritise.

Background

In May 2023, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (the Ad Hoc Committee), released the Draft text of the Convention (the Zero Draft).[1] The Zero Draft represents elements negotiated during the fourth and fifth sessions, and is still open to proposals during the ongoing negotiation process. This Zero Draft is structured into nine chapters, prefaced by a preamble of framing principles.[2] It is scheduled to be discussed at the forthcoming sixth session of the Ad Hoc Committee, commencing on 21 August 2023 in New York.

[1] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft text of the convention, A/AC.291/22, 29 May 2023.

[2] **Chapter I** begins with a statement of purpose and key definitions. **Chapter II** delineates new substantive offences in Articles 6 through 16 that are later explicitly referenced in the Draft Text. Article 17 also calls for the implementation of additional non-cyber dependent offences, but is *not* subject to the same stipulations and protections as Articles 6 through 16 (more on this below). **Chapter III** defines the scope of jurisdiction of the Convention, which extends explicitly beyond the substantive offences of Articles 6 through 16 and beyond cybercrime generally. **Chapter IV** outlines procedural measures and law enforcement powers, providing for the scope of data requests, and real-time data collection. **Chapter V** provides for international cooperation, including in matters of data sharing and extradition; **Chapters VI and VII** outline preventative measures and encourage data and technical exchange, respectively. **Chapters VIII and IX** contain implementation, logistical, and final provisions.

ARTICLE 19 has already provided guiding principles on the substantive offences in Chapter II of the Negotiating Document.[3] In this analysis we focus specifically on the ambiguities of scope of the proposed Convention, the lack of human rights and due process safeguards, and the potential implications of law enforcement powers on emerging surveillance and policing technologies.

ARTICLE 19 reiterates our earlier concerns about the need of an international instrument on mutual legal assistance where parallel regional instruments have been recently passed to provide for such frameworks. This includes the Second Optional Protocol to the Budapest Convention which has been internationally adopted beyond the European community. As such, the effectiveness of international, rather than regional or bilateral, standards on mutual legal assistance is unclear, given the widely ranging strength (or even existence of) fundamental data protections at the State level.

ARTICLE 19's key concerns with the Zero Draft are as follows:

1. The Convention explicitly criminalizes and allows data-sharing, without limitation, for offences beyond its scope;

2. Human rights and procedural safeguards, including proportionality, notice, and rights of independent review, are either non-existent or optional;

3. The Convention is silent on whether it allows sharing of artificial intelligence datasets, biometrics, or other large-scale databases which enable surveillance, predictive policing, and the restriction of privacy tools or blockchain;

4. The Convention still contains content-related offences that are unnecessary or may lead to bans of books or otherwise infringe freedom of expression online.

1. Explicit criminalization and allowance of data-sharing, without limitation, for offences beyond the scope of the Convention

The scope of offences in Zero Draft extends beyond Articles 6 through 16

While the Zero Draft initially appears to define a finite number of substantive offences in Articles 6 through 16, language throughout the Convention indicates the scope is far from limited to those offences. Indeed, the scope is explicitly open-ended. We are particularly concerned about the provisions of Article 17, which requires State Parties to ensure that:

[3] These guiding principles are threefold: cybercrime offences must require dishonest intent, serious harm, and be cyber dependent rather than cyber-enabled.

> [O]ffences established in accordance with applicable international conventions and protocols also apply when committed through the use of [a computer system] [an information and communications technology device]

Nowhere are "applicable international conventions" specified, limited, or otherwise defined.

ARTICLE 19 appreciates that the drafting process has made some progress in eliminating substantive offences that are "cyber-enabled" rather than "cyber-dependent" (i.e. offences requiring the use of a computer system, rather than traditional offences committed using a computer). However, Article 17 undermines any substantive shift of the Convention to cyber-dependent offences, explicitly allowing for additional offences merely "when committed through the use of" a computer system.

We also note that the Preamble frames the Convention to address cyber-enabled offences "related to terrorism, trafficking in persons, smuggling of migrants, illicit manufacturing of and trafficking in firearms." Several of these offences appeared in the last Negotiating Document and were removed (previous Articles 29-31).[4] States explicitly chose not to include these offences in the Zero Draft, and as such they should not be introduced again in a backdoor fashion.

Recommendations:

- As of this stage of the drafting process, the Zero Draft makes clear that there is still not consensus as to the underlying scope of either its substantive criminal provisions or mutual legal assistance. Therefore, we encourage States to explicitly define the scope of both prongs of the Convention before proceeding into further negotiations.
- The reference in the Preamble to offences that are not in the Convention should be stricken, as this only creates confusion and ambiguity as to the scope of the Zero Draft.
- Article 17 should be stricken in its entirety. If State Parties cannot agree to strike it, Article 17 must at a minimum be amended to apply *only* to cyber-dependent offences. We suggest changing "when committed through the use of" to "when dependent on the use of" a computer system.

Encouraging information and data-sharing beyond cyber-dependent offences in mutual legal assistance provisions

ARTICLE 19 is concerned that several mutual legal assistance provisions contemplate potentially limitless application beyond the scope of the Convention. In particular:

[4] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/16, 7 November 2022.

- The scope of procedural measures in Article 23(2) apply not only to the offences of Articles 6 through 16, but to "other criminal offences committed by means of a computer system" and the collection of evidence in electronic form for "any criminal offence."

- Mutual legal assistance is defined broadly in the "widest measure" in Article 40—the very first paragraph references Article 17, directing States to provide assistance for "serious crimes" as well as "offences covered by article 17."

- Transmitting of information provided in Article 40(4) is allowed for any "information relating to *criminal matters*" generally, rather than criminal provisions of the Convention.

- Mutual legal assistance requests—for instance real-time collection of traffic data (Article 45(3)(c))—explicitly contemplate requests for an "offence *or other illegal act*."

- Article 47(1), providing for law enforcement cooperation, directs State Parties to conduct inquiries into offences "covered by this Convention," rather than offences specifically enumerated in Articles 6 through 16. The same section also encourages sharing of "data for analytical or investigative purposes," meaning data sharing would not be confined to those Articles.

- Article 49(1)(b) directs State Parties to permit authorities to order the confiscation of property involved in offences under the Convention, using the domestic offence of money-laundering or "other procedures authorized under its domestic law."

- Article 49(2)(c) directs State Parties to "Consider taking additional measures to permit its competent authorities to preserve property for confiscation, *such as on the basis of a foreign arrest or criminal charge* ***related*** *to the acquisition of such property*." Such arrests and criminal charges merely need to be "related" to acquisition of property, potentially extending beyond offences of the Convention (or even a computer system).[5]

ARTICLE 19 is concerned that the open-endedness of scope of mutual legal assistance will inevitably lead to asymmetries in application. We further note that dual criminality is *not* a requirement for providing assistance (see Article 40(8)). It is merely optional; State Parties "may decline" on the absence of dual criminality. This means that the only safeguard that exists where States have varying manners of implementation are the decisions of States to provide assistance. The privacy and due process protections of individuals will thus vary depending on the requested State and the strength of their domestic protections.

Recommendations:

- Provisions in Article 23(2)(b) and 23(2)(c), allowing for mutual legal assistance beyond cyber-dependent offences or cybercrime offences at all, should be stricken entirely.

[5] While this Article depends upon a request made pursuant to Article 50(2), which would be tied to offences under Articles 6 through 16 of the Convention, the "additional measures" are not similarly restricted.

- The last clause in Article 40(1) should be stricken, removing reference to "serious crimes" and Article 17.
- Article 40(4) should replace "information relating to criminal matters" with "information relating to violations of Articles 6 through 16."
- Article 45(3)(c) should replace "offence or other illegal act" with "offence under Articles 6 through 16."
- Article 47(1) should replace "covered by this Convention" to "under Articles 6 through 16."
- Article 49(1)(b) should be amended to strike "other procedures outlined under its domestic law."
- Article 49(2)(c) should be stricken entirely.

2. The lack of human rights and procedural safeguards, including proportionality, notice, and rights of independent review

ARTICLE 19 finds that the Zero Draft suffers from a dangerous asymmetry, where procedural protections only apply to a fraction of the offences it establishes, and are virtually non-existent with regard to mutual legal assistance and sharing of user data. Further, the procedural safeguards provided in Article 24 are only articulated to apply to Chapter IV, not to Chapter V, which lays out significant cooperation and data-sharing.

We begin by noting positively that Article 21(4) requires State Parties to ensure that individuals prosecuted under Articles 6 through 16 enjoy protections "consistent with the obligations of the State Party under international human rights law, including the right to a fair trial and the rights of defence." Further, Article 21(1) requires sanctions to be "proportionate," and other provisions under Article 21 provide for due process rights. Article 5 of the Convention also explicitly references international human rights obligations. These are necessary and important statements.

The fatal problem, however, is that Article 17, which also implements substantive offences, is nowhere mentioned in Article 21, meaning that the Convention would appear not to require those protections for offences established under Article 17. It is unclear whether this is an oversight or deliberate. Further, Articles 6 through 16 only cover a fraction of offences under which mutual legal assistance might be provided, as outlined above. This means that the Convention outlines mutual legal assistance for a wide range of offences that have no explicit due process limitations at all under the Convention.

It is strange and glaring that the Zero Draft provides due process in Articles 6 through 16, but not for all offences it provides. Meanwhile, the Zero Draft still allows mutual legal assistance and evidence collection in cases where those same protections are not guaranteed. As a result, States may find themselves complicit in the following investigations and prosecutions:

- Offences that are not guaranteed to have proportionate sanctions;

- Trials that are not inherently fair or have a right to defence;
- Prosecutions that do not feature fair or humane standards of detention.

Although Article 24(1) indicates that the establishment, implementation and application of the powers and procedures under the respective section shall "incorporate the principle of proportionality," but we observe that this is a weaker statement than Article 21 where sanctions must explicitly be proportionate. Any further safeguards included in the Convention are discretionary and optional, and relegated to domestic law, which may include jurisdictions that may have not ratified core international human rights treaties or regional instruments guaranteeing fundamental due process rights.

Recommendations:

- To the extent that terms such as "data" and "information" are used, they must be defined in Article 2 of the Convention. For example, it is unclear whether "information" references "subscriber information" or is intended to be construed more broadly. These terms are used in Articles 40(4), 40(30)(b), and 47(1)(c), for example, but are not presently defined.
- Article 21 must be amended to include Article 17 in its procedural protections, should Article 17 remain in the Convention (we maintain that Article 17 should be stricken entirely).
- Article 21 must be amended to apply not only to substantive criminal provisions, but also to predicate offences for mutual legal assistance requests, such that requests are only made for investigations and proceedings where there is a guarantee of proportional sanctions, a fair trial, and procedural safeguards consistent with international human rights law.
- Article 21 must articulate the fundamental safeguard of notice and access to data, including the manner in which data is shared or utilized across jurisdictions or to any third parties or private entities.
- Article 24 should be amended to apply to "this chapter and Chapter V."
- Article 24(2) should strike the clause "as appropriate in view of the nature of the procedure or power concerned."

Absence of protections for voluntary data sharing, notice to users, or retention limits

ARTICLE 19 is deeply concerned that the Zero Draft explicitly endorses and encourages the sharing of "data" across jurisdictions without specifying what that data entails. Article 47(1)(c) directs that State Parties "shall cooperate closely with one another" to "provide, where appropriate, necessary items or data for analytical or investigative purposes." Notably, this provision is not tied to specific investigations or law enforcement proceedings as are other mutual legal assistance provisions in the Convention. It also does **not** define what type of "data" might be shared pursuant to the definitions in Chapter I, Article 2. As such it is unclear whether this means that "personal data," "traffic data," or other forms such as metadata might be shared without a particularized assistance request. A similar provision appears in Article 40(4), which allows a State to share, without a formal request, "information relating to criminal matters"

where they merely "believe" such information could "assist" the authority. Similarly, it is nowhere defined what "information" means here.[6]

At the same time, the Zero Draft does not provide meaningful rights to users on data that is shared with third parties and international organizations, pursuant to Article 36(3). One of the only safeguards appears in Article 36(2), which provides for personal data transferred to be "subject to effective and appropriate safeguards in the respective legal frameworks of the State Parties."[7] This does not provide for consistent and binding procedural safeguards under international human rights law.

The Zero Draft is silent on retention and notice to users. Indeed, notification appears in Article 42(g), but in the context of a request to keep a preservation request "confidential" and "not to notify the user." The prohibition on notice appears indefinite; indeed, individuals have no way of knowing the full extent of the sharing of their data pursuant to the Convention, and as such, can have no meaningful right of independent review or remedy of violations. There are no articulated retention or deletion periods, rights of deletion, or other procedural safeguards; the closest mentions of safeguards are effectively optional.[8]

Recommendations:

- Article 36(1), on the protection of personal data, should strike the word "applicable," as international human rights standards are universal, binding, and not subjective.
- Article 36(2), on the protection of personal data, should be amended to read "safeguards in the respective legal frameworks of the State Parties and international human rights law."
- Article 47(1)(c) should be stricken, as it allows for generalized data sharing without restriction or notice to users.
- Article 42(g) should be amended to provide a limitation on the duration of not notifying a user of a preservation request.
- The substantive offences of Chapter II should include an explicit right to a public interest defence.

[6] See also Article 40(30)(b) which allows a requested State Party to provide "copies of any government records, documents or information" which are "not available to the general public." It is not defined what "information" means in this context.

[7] While Article 40(19) appears to restrict transmitting or use of information for "investigations, prosecutions or judicial proceedings" beyond those requested, this restriction appears to only apply to formal mutual legal assistance (rather than voluntary data sharing pursuant to cooperation), and is overcome by written consent of the requested State.

[8] The closest restriction appears in Article 24(2), which indicates that safeguards shall include "limitation of the scope and the duration of such power or procedure." However, the same provision is limited "as appropriate in view of the nature of the procedure or power concerned," which is subject to individual State interpretation rather than any oversight or international standards. As such, in practice this procedural protection is effectively optional.

Wide scale of undefined public-private partnerships not constrained by jurisdiction and without user procedural protections and notice

In numerous instances, the Zero Draft heavily contemplates public-private partnerships in terms of not only training, but active "prevention" as well as sharing of user data. ARTICLE 19 observes that the private sector and stakeholders referenced do not need to be in the same jurisdiction, providing a gaping potential backdoor to the whole mutual legal assistance process.

These ambiguities are particularly problematic given that there are no indications that users of private platforms or services have a right to be notified or enjoy basic protections. Some instances of those partnerships include:

- Article 53 provides for a broad coalition to be engaged for the purposes of "active participation" in "prevention" of offences "covered" by the Convention (note that "covered" may not mean specifically defined). This coalition explicitly includes the "private sector."
- Article 53 also explicitly defines "preventive measures" to include "strengthening cooperation" with "relevant stakeholders."
- Article 54(4) directs States to "leverage" and "cooperate closely" with the private sector among other actors.
- Article 54(6) directs States to create "strategies and action plans" to "prevent and combat" cybercrime.
- Article 55 directs States to analyse "trends" in cybercrime with the private sector.
- Article 56(2)(d) encourages States to work with the private sector to provide technologies and "modern equipment" to developing countries to combat cybercrime.
- Article 36(3) provides for the sharing of information with third countries and international organizations, which are nowhere defined or elaborated on in the Zero Draft. That sharing is subject to no further limitations once in the possession of those third-party entities.
- Article 24(3) directs States to consider the impact of powers on "the rights, responsibilities and legitimate interests of third parties" without specifying who those third parties are.

ARTICLE 19 observes that historically, public-private partnerships for the "prevention" of cybercrime may involve efforts to install backdoors into software, malware onto devices, or provide governments the ability to surveil the activity of users without even requiring mutual legal assistance requests. This allows for an effective backdoor around the mutual legal assistance procedures wherein private actors may simply agree to share data for "preventive" reasons that are not even subject to the minimal procedural protections of the Convention.

Recommendation:

- Articles 53 and 54 should be amended to clarify the parameters of public-private partnerships, and provide transparency and recognize the rights of users to be notified regarding the extent that private actors are cooperating with State actors.

Absence of independent and judicial review

For such a far-reaching and comprehensive Convention, ARTICLE 19 is surprised that the words "judicial or other independent review" appear only once in the whole Zero Draft – only in Article 24(2). In the instance where it appears, it is limited to inclusion "as appropriate." Otherwise, safeguards are relegated throughout the Convention to the domestic law of State Parties. Where those domestic laws do not align with international standards, this is particularly problematic.

Recommendation:

- The Convention must include an absolute right of independent review.

3. The Convention's lack of clarity over sharing of artificial intelligence datasets, biometrics, or other large-scale databases

ARTICLE 19 highlights that the aforementioned data-sharing provisions are especially and urgently problematic in light of the stakes of current and emerging technologies. As noted, numerous cooperation provisions in Chapter V contemplate the sharing of data without a predicate assistance request or even the need for an ongoing investigation. Several articles, including Articles 40(4), 40(30)(b), and 47(1)(c), use terms such as "data" and "information" which are not explicitly defined, and it is unclear whether they refer to individualized data or could refer to entire databases.

This is critical to define with precision as seemingly innocuous terms such as "information" might actually cover the sharing of **billions** of user records, **terabytes** of biometric databases or **artificial intelligence training datasets**. These concerns are neither hypothetical nor speculative; the use of these tools rank among the highest global law enforcement trends and priorities. In June 2023, INTERPOL and the United Nations Interregional Crime and Justice Research Institute (UNICRI) met in Singapore to discuss the use of artificial intelligence and provided a "Toolkit for Responsible AI Innovation in Law Enforcement." In convening, the group acknowledged that "law enforcement agencies are already making extensive use of AI systems."[9] Indeed, the Toolkit features a comprehensive guide on data collection and the types of data desired for useful data-sets.

> Data plays a central role because it is the raw material which machine learning models use to operate. In other words, machine learning models process large amounts of data in order to carry out functions such as recognising patterns in the data, patterns that can then be used to make predictions about new data points.[10]

[9] INTERPOL and UNICRI release blueprint for responsible use of AI by law enforcement, 8 June 2023.

[10] UNICRI and INTERPOL, Toolkit for Responsible AI Innovation in Law Enforcement: Technical Reference Book, June 2023, p. 36.

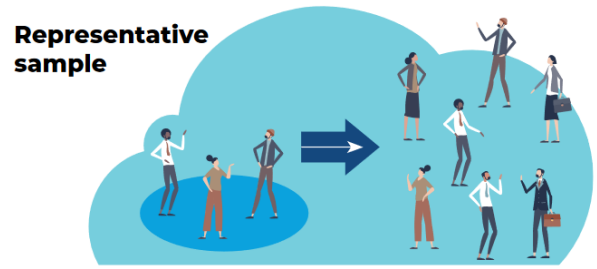

Figure 20 - How to select a representative sample of the population to have good quality data.

38

Excerpt from "Technical Reference Book" from the AI Toolkit

We observe that it is positive that agencies are attempting to address ethical implications of the use of artificial intelligence; however, this is not the case globally, and certainly will not be the case of all actors that would be subscribing to the Convention.

ARTICLE 19 specifically notes that technologies such as facial recognition, voice recognition, and biometrics, which rely on large data-sets and artificial intelligence, can be and have been used at scale for purposes of repression, surveillance, and dissent.[11] These cases are well-documented, but it is still ambiguous the extent to which the Convention allows for sharing of the underlying data that enables such abuses on freedom of expression, association, and fundamental freedoms.

Problematic encouragement of information-sharing to scrutinize the use of privacy tools

Finally, ARTICLE 19 draws attention to Article 47(1)(d) which provides for the "exchange" of "information" concerning "specific means and methods used to commit the offences covered by the Convention." This, specifically, refers to "other means of concealing activities" including "techniques and procedures" on computers.

ARTICLE 19 is concerned that the language of Article 47, encouraging information-sharing related to "concealing activities," will provide a pretext to investigate and serve to stifle the very means that human rights defenders, journalists, dissidents, and civil society use to exercise their rights to freedom of expression online. Other provisions that suggest cooperation which could stifle freedom of expression and privacy tools include sections on preventive measures, such as Article 53(3)(a) which encourage "cooperation" between law enforcement and "stakeholders" (potentially the private sector). Some of these technologies include, but are not limited to, the

[11] D. Litvinova and G. Stachel, How Russia Controls Information, Watches Citizens, Voice of America, 30 May 2023; Z. Lampell, The Impact of Artificial Intelligence Technologies on the Right to Privacy and Civic Freedoms, International Center for Not-for-Profit Law, 28 May 2021; or P. Gill, India is ramping up the use of facial recognition to track down individuals without any laws to keep track of how this technology is being used, Business Inside India, 10 Feb 2021; Mara Hvistendahl, How a Chinese AI Giant Made Chatting—and Surveillance—Easy, Wired, 18 May 2020.

use of end-to-end encrypted chat services (such as Signal or WhatsApp), anonymous browsers, or routing tools such as VPNs and TOR (The Onion Router), which routes Internet traffic through nodes globally. Some of these tools are necessary for individuals in some States to have meaningful access to the Internet. International human rights law is clear that encryption and anonymity tools are crucial to the exercise of freedom of expression online. As such, restrictions on the use of these tools must be analysed in terms of the tripartite test on restrictions of freedom of expression.[12]

ARTICLE 19 has also previously outlined the relationship between blockchain and cryptocurrency, and freedom of expression.[13] We are concerned that the use of accessory or aiding and abetting offences, such as in Article 16(1)(b)(ii) covering property involved in money laundering, could be abused to criminalize or shut down cryptocurrency platforms. This problem is analogous to the reason that social media providers, or content creation platforms, frequently enjoy protection from liability for the activities of users on their platforms so long as the platforms are content-neutral.

Recommendations:

- The Convention should specifically address whether or not the sharing of large-scale datasets for artificial intelligence, biometrics, or similar purposes is permitted under the definitions of "data" and "information."
- Article 47(1)(d) should be amended to clarify that the lawful use of privacy technologies will not be investigated or scrutinized. In the alternative, Article 5 of the Convention, Article 21, or Article 53 should be amended to include specific language affirming that the right of individuals to use privacy-enhancing tools will be respected and protected through cooperation protocols.
- Article 16 should be amended to include protection from money laundering charges against blockchain or cryptocurrency platforms that are content-neutral and do not have specific, dishonest intent to participate in illegal activities.

4. Unnecessary content-related that may infringe freedom of expression online

Child exploitation offences and criminalization of "written material"

ARTICLE 19 observes that Article 13 of the Zero Draft outlines offences related to child sexual abuse and exploitation material. ARTICLE 19 notes that the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography[14] defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."

[12] See e.g. ARTICLE 19, Report: The Right to Online Anonymity, 18 June 2015.
[13] ARTICLE 19, Blockchain and freedom of expression, 2019.
[14] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, adopted on 25 May 2000 by Resolution A/RES/54/263 at the 54th session of the UN General Assembly.

As 176 States are already parties to the Protocol, which provides for mutual investigative assistance, ARTICLE 19 reiterates its question about whether a cybercrime treaty is a necessary place to impose additional content-based obligations.

ARTICLE 19 also observes that Article 13(2)(b) defines "material" to include not only "images" but also "written material." It is not clear the limits of what written material include, and whether this could give rise to the banning or sale of books. Note, for instance, that there exist world-wide best-selling novels (such as the Song of Ice and Fire series by George R.R. Martin, famously adapted to the Game of Thrones television series) that frequently describe or depict brutal acts as part of their story, including sexual abuse of children.[15] These are far from fringe works; novels have been translated into 47 languages, sold nearly 100 million copies worldwide, and adapted into one of the most popular television series globally of all time.[16] Part of the appeal of the stories for many is the grim social commentary they provide on war and history. Nevertheless, criminalizing the possession or sale of this book would appear to be encouraged by the text of Article 13.

The Article appears to address this by offering optional protections for expression in Article 13(3), allowing states to limit laws to instances featuring a real child or visual depictions. We are concerned that given the discretionary nature, this section does not provide a strong enough protection against infringements on artistic or literary expression.

Recommendations:

- Given the widespread ratification of the Optional Protocol to the Convention on the Rights of the Child, we question the added necessity of this Article.
- Article 13(3) should be amended to be compulsory, limiting criminalization of materials to real children or visual representations, rather than written materials, which could have the effect of banning books.

Non-consensual sharing of intimate images without defining "sexual activity"

While non-consensual sharing of images is an extremely problematic phenomenon, ARTICLE 19 believes that addressing it in an international criminal instrument raises serious and complex issues in balancing freedom of expression and privacy rights. The issue presented in Article 15 is one of personal privacy, fundamentally distinguishing it from other offences, and featured in existing regional instruments such as the Budapest Convention. The subtext for these prohibitions is protecting the privacy rights of victims; privacy rights are outlined in human rights instruments and data protection mechanisms. Thus, we maintain that these provisions must be analysed under these frameworks.

[15] Rape in ASOIAF vs. Game of Thrones: a statistical analysis, Tumblr Post, 24 May 2015 (warning: graphic written descriptions).

[16] Robin Dunbar, Science reveals secrets behind the success of Game of Thrones, Oxford News Blog, 3 Nov 2020.

While the provision has been scaled back in the drafting process, we still note that existing terminology is vague and open to subjective interpretation, exposing it to abuse. As drafted, we are concerned that these provisions may inadvertently create problematic violations or be misused through provisions that are subject to widely varying interpretations. For example, Article 15(2) includes in the definition of an "intimate image" a person that is either nude *or* "engaged in sexual activity." Definitions of "sexual activity" may vary greatly, depending on the area and customs. It is not clear whether kissing may amount to sexual activity in some jurisdictions. Worse, these terms could be interpreted to discriminate against same-sex interactions, which have historically been targeted under obscenity and pornography laws.

Existing human rights instruments and data protection mechanisms already address questions of personal privacy, and a cybercrime treaty where these conversations are not taking place is not the proper venue to consider them. We also believe that civil mechanisms, national oversight bodies, as well as regional instruments, could be more appropriate venues to consider. This is particularly important given that "intent to cause harm" is merely optional under Article 15(3).

This issue is compounded in jurisdictions where there has already been a push to criminalize pornography generally. For example, regional instruments such as the problematic Arab Convention on Cybercrime broadly call for punishment of pornography; where this is the case, terminology like "sexual activity" may be interpreted in sweeping manners.

Recommendations:

- Article 15 should be stricken in its entirety. At a minimum, vague terminology such as "sexual activity" should be stricken or very narrowly defined.