Privacy International's Briefing on the Draft Text of the UN Cybercrime Convention (version as of 1 September 2023)

September 2023

Introduction

In this briefing Privacy International (PI)[1] outlines its analysis of some key provisions on the draft text of the UN Cybercrime Convention[2], with the aim to provide delegations of Member States and other stakeholders with our recommendations to strengthen the draft and bring it into line with human rights law. This briefing builds upon the submissions made by PI at the previous sessions of the AHC and reflects upon some of the amendments proposed by Member States. While not aiming to be comprehensive, it covers in particular the following Articles: 2, 3, 5, 23, 24, 28, 29, 30, 35, 36, 47 and 54.

While we recognise the threats posed by cybercrime, we remain deeply concerned about certain provisions in the current draft and how these might be misused to undermine human rights. These concerns are shared by UN independent human rights experts and non-governmental organizations who have reported on the abuse of cybercrime laws. PI wishes to emphasise the need both for a narrow scope for the proposed Convention, focusing solely on core cyber-dependent crimes, as well as for safeguards throughout the entire treaty to ensure human rights are protected, especially in the areas of privacy and freedom of expression. Additionally, we are worried about the potential misuse of provisions relating to surveillance and data collection, and call for stringent safeguards to prevent abuse. We urge States to ensure that the treaty does not become a tool for governments with a poor human rights record to justify human rights abuses under the guise of combating cybercrime.

Chapter I - General provisions

PI believes that cybercrimes can pose a threat to the enjoyment of human rights. At the same time, we are concerned that cybercrime laws, policies, and practices are currently being used to undermine human rights. We are not alone to raise this concern. Several UN independent human rights experts and non-governmental organizations have reported on the human rights abuses stemming from overbroad cybercrime laws. For example, the Office of the High Commissioner for Human Rights has raised concerns about "*the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly.*"[3] In a similar vein, in 2021 the UN General Assembly expressed grave concerns that cybercrime legislation was "*in some instances misused to target human rights defenders or have hindered their work and*

[1] Privacy International (PI) is a non-governmental organization in consultative status with ECOSOC. PI researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilizes allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

[2] See Draft Text of the Convention as of 1 September 2023, reflecting comments of Member States: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf

[3] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf.

endangered their safety in a manner contrary to international law."[4] It is therefore essential to keep the scope of the proposed Convention narrow to core cyber dependant crimes. Otherwise, the Convention risks becoming an instrument that justifies states' violations of human rights.

Similarly, the Convention should clarify that any procedural measures and law enforcement cooperation (including in relation to the collection and transfer of evidence) should be limited to addressing only the core cybercrimes as included in the Convention and not the full range of criminal conduct, to avoid investigative powers and procedures being used for less serious crimes or crimes that may not be consistent with States' human rights obligations. The proposed Convention is about addressing cybercrime, not a general-purpose law enforcement treaty.

PI recommends that:

- **Article 2** is amended to define cybercrime as offenses in which information and communications technologies (ICTs) are the direct objects as well as instruments of the crimes (cyber-dependant crimes, i.e., crimes that could not exist at all without the ICT systems);
- **Article 3** is amended to limit the scope of application of the Convention to the prevention, detection, investigation and prosecution of the cybercrimes included in the Convention, as well as the collecting, obtaining, preserving, and sharing of evidence in electronic form for cybercrimes as included in the Convention.

PI welcomes the provision in **Article 5** on respect for human rights and the inclusion of gender perspectives. However, we note the need to include that specific safeguards to ensure the respect of human rights is included in other provisions of the proposed Convention (see comments below.) Failure to reflect these safeguards risks creating a disconnect between the general obligation under Article 5 and those contained in other articles of the Convention — a disconnect that risks creating legal uncertainty and that can be exploited by those governments seeking to justify laws and practices that do not comply with human rights.

With regards to Article 5(1), PI:

- Supports the proposal to include the phrase "in accordance with international human rights law" in Article 5(1);
- Recommends including a reference to the principles of legality, necessity, proportionality, transparency, oversight and access to remedies in Article 5(1).

Chapter II – Criminalization

As noted in the observations under Chapter I above, the scope of criminal conduct covered under the definition of 'cybercrime' should be narrow, precise, and specific. It follows that this chapter should only cover core cyber dependant crimes, i.e., offenses in which ICTs are the direct objects as well as instruments of the crimes; these crimes could not exist at all without the ICT systems.[5]

Further, criminal conduct, such as illegal access, should require criminal intent and harm. Standards such as "without authorization" or "without right" risk allowing the criminalisation of acts carried out with beneficial intent, such as security research, and increase the likelihood

[4] See https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/427/11/PDF/N1942711.pdf?OpenElement.
[5] A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention: illegal access to computing systems, illegal interception of communications, data interference, system interference, and misuse of devices. For example, spreading a computer virus in the wild, breaking into the computer system of a bank to steal money, and using malicious software to delete all the data of a former employer's systems.

of prosecuting individuals for behaviour that did not, or could not have been expected to, cause any harm or damage.

For these reasons, PI recommends that:

- Only cyber dependant crimes are included in the Convention text, as those covered in **Articles 6 to 10**;
- The standards of criminal intent and harm are introduced in the Convention text.

Should other non-cyber dependent crimes be included, PI recommends that cyber-enabled crimes are narrowly defined and consistent with international human rights standards. The Convention should not seek to cover ordinary crimes already clearly and adequately prohibited under existing domestic legislation and merely incidentally involving or benefiting from ICT systems without targeting or harming those systems.

Additionally, PI is particularly concerned about the proposals to include "extremism-related offenses" (**Article 15 quinquies**), "terrorism-related offenses" (**Article 15 septies**) and "acts threatening public safety" (**Article 15 duodecis.**) There are no internationally agreed definitions for those crimes and many states justify human rights repressive practices, such as the prosecution of political opponents, human rights defenders, and journalists, the unlawful restriction of the exercise of the rights to freedom of expression and peaceful assembly, and the unlawful interference with the right to privacy, on the basis of broad, ill-defined crimes under their national legislation.

Chapter IV - Procedural measures and law enforcement

Widening the scope of this Chapter to cover all crimes committed with the use of an ICT significantly risks undermining human rights, including the right to privacy and the right to a fair trial. As the 2022 UN Security Council's Counter-Terrorism Committee Executive Directorate noted, in attempting "*to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process*."[6]

For the reasons illustrated in our comments on Chapter I above, PI recommends that the scope of procedural measures is limited to the investigation of the criminal offenses established in accordance with this Convention.

With regards to Article 23, PI:

- supports the proposal to include 'specific' in **Article 23(1)**. This proposal ensures that the powers conferred under this chapter are employed exclusively for specific and targeted criminal investigations or proceedings. As such, it reaffirms the commitment to uphold the principles of legality, necessity and proportionality in exercising these powers;
- recommends that **Article 23(2)(a)** reads: "the criminal offences established in accordance with articles 6 to 10 of this Convention", for the reasons expressed above (see Chapter I on scope of the Convention);
- supports the proposal to delete **Article 23(2)(b)**, for the reasons expressed above (see Chapter I on scope of the Convention);
- supports the proposal to limit **Article 23(2)(c)** to the collection of evidence of criminal offences established in accordance with articles 6 to 10 of this Convention. Without

[6] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), The state of international cooperation for lawful access to digital evidence: Research Perspectives, January 2022, available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf

such limitation, **Article 23(2)(c)** may allow for the use of any investigatory power and procedure established by the Convention for the prevention or detection of any offence. This not only widens the scope of the Convention beyond the offences it is meant to cover, but it also raises compatibility issues with international human rights standards, such as necessity and proportionality. It could potentially allow law enforcement authorities to use measures that seriously interfere with individuals' right to privacy or free expression to, for example, prosecute petty offenses or criminal offenses, including content-related offenses, which are inherently inconsistent with States' human rights obligations.

With regards to Article 24(1), PI supports:

- the proposal to amend **Article 24(1)** to extend the application of this provision to the whole Convention (and not to limit it only to chapter IV);
- the reference to international human rights law;
- the proposals to include the principles of legality, necessity and proportionality.

The principle of legality is a fundamental aspect of international human rights instruments and the rule of law in general. It is an essential guarantee against the state's arbitrary exercise of its powers. Second, the principle that any interference with a qualified right, such as the right to privacy or freedom of expression, must be necessary and proportionate is one of the cornerstones of international human rights law.[7] In general, it means that a state must not only demonstrate that its interference with a person's right meets a "pressing social need," but also that it is proportionate to the legitimate aim pursued.

With regards to Article 24(1), PI recommends that:

- the Article is amended to require that "a factual basis justifying access or application of powers" to ensure that any access or application of these measures is based on objective and verifiable facts, rather than arbitrary, biased or speculative reasons.

With regards to Article 24(2), PI:

- recommends that the qualifier "*as appropriate in view of the nature of the procedure or power concerned*" in Article 24(2) is deleted to clarify that the conditions and safeguards expressed in this article apply to all procedures or powers provided in the Convention;
- recommends that **Article 24(2)** is strengthened to require not only independent supervision but also prior independent (preferably judicial) authorisation of surveillance measures that interfere with the right to privacy. Any independent (preferably judicial) authorization of surveillance powers should be prior to the exercise of those powers. This is to provide the necessary degree of independence and objectivity to prevent the abuse of surveillance powers. Such safeguard serves as an extra layer of protection to prevent potential abuses, enhancing accountability and upholding the rule of law. As the European Court of Human Rights has repeatedly emphasized, the safeguard of prior judicial authorisation serves "*to limit the law-enforcement authorities' discretion,*" by establishing a practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case.[8] This would bring the paragraph in line with existing jurisprudence of human rights courts and bodies;[9]
- supports the proposal to include of the right to an effective remedy in **Article 24(2)**. As noted in the report of the UN High Commissioner for Human Rights 'The right to privacy

[7] For a compendium of relevant international and regional human rights standards, resolutions and jurisprudence, see Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance.
[8] ECtHR, *Szabó and Vissy v Hungary*, App No 37138/14, para 73.
[9] See Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

in the digital age', effective remedies for violations of privacy "*must be known and accessible to anyone with an arguable claim that their rights have been violated.*" In particular, the High Commissioner stated that "*notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy.*" Further, the effective remedies must include "*prompt, thorough and impartial investigation of alleged violations*" and such independent investigative bodies need to have the power to order the end of ongoing violations as well as "*full and unhindered access to all relevant information, the necessary resources, and expertise to conduct investigations and the capacity to issue binding orders.*"[10] We also recommend the inclusion of adequate notification to ensure individuals are informed when their rights are affected by the powers and procedures outlined in this Chapter. Notification allows individuals to exercise their rights to an effective remedy;[11]

- recommends that **Article 24(2)** requires the "*periodic disclosure of statistical data on the use of powers and procedures*". This proposal would enhance transparency and accountability, making it mandatory for States Parties to periodically disclose statistical data on how they are using their powers. It ensures that states are not using their powers excessively or inappropriately, and allows for public scrutiny and debate, furthering democratic values.

As far as **Article 28** (Search and seizure of [information stored or processed electronically] [stored computer data]) is concerned, its wording raises concerns about any potential obligations imposed upon third parties, such as communication services providers, to either disclose vulnerabilities of certain software or to provide relevant authorities with access to encrypted communications. It should be noted that, if authorities are allowed to exploit such gaps, they will more likely than not have an interest in building an "arsenal" of security gaps to be able to attack a target in the event of an investigation. This interest, in turn, will prevent them from notifying the affected manufacturer of IT systems, who can help close the security gap that has been discovered. If this happens, it means that the worldwide security risk would far outweigh the possible facilitation of prosecution in individual cases. Moreover, requirements imposed on service providers that would essentially compromise existing security standards in communications might equally constitute a serious interference with, among others, the right to privacy. International human rights law requires states to abstain from such interferences or even take measures to ensure a high level of security, integrity, and confidentiality of communications within the context of their positive obligations.

PI recommends:

- the deletion of **Article 28(4)** for the reasons stated above.

As far as **Article 29** (Real-time collection of traffic data) and **Article 30** (Interception of content data) are concerned, we wish to underline that real-time collection of traffic data and interception of content data are extremely intrusive measures, to be applied only for serious crimes, following a prior judicial authorisation that assess their necessity and proportionality, including whether other less privacy intrusive measures were not available to achieve the legitimate aim. PI is therefore concerned by the proposal to include these powers in this Convention as the risk of abuse is very high.

For these reasons, PI:

- Supports the proposals to delete **Article 29** and **Article 30**.

Should these Articles be retained, PI:

[10] See UN Doc A/HRC/27/37.

[11] See UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020) and Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014), paragraph 40.

- Supports the proposal contained in the working document of Working Group 6 to replace 'shall' with 'may' in **Article 29(1)** and **Article 30(1)**;[12]
- Recommends including in paragraph 1 of **Article 29** and **Article 30** the wording: "With regard to the criminal offences established in accordance with articles 6 to 10 of this Convention";
- Recommends including requirement of prior judicial authorisation and that the collection of content traffic data and the interception of content data is only conducted when "there is reasonable belief that a criminal offense was committed or is being committed";
- Recommends that **Article 29(3)** and **Article 30(3)** include a qualifier such as "only to the extent that such confidentiality is needed in order not to prejudice an ongoing investigation" to prevent being used to justify measures that prevent accountability and access to remedies.

As far as **Article 30bis** and **Article 30ter** (Admission of electronic evidence) are concerned, their current wording is very broad and provides no meaningful safeguards to ensure that the evidence collected and admitted complies with international human rights law, including the right to a fair trial and the right to privacy. This is a significant gap given the practices of some states to extract evidence from people's personal devices in ways that are unregulated. For example, PI documented how mobile phone extraction tools enable police and other authorities to download content and associated data from people's phones.[13] This can apply to suspects, witnesses, and even victims of crime – often without their knowledge or consent.[14] Increasingly mobile phone extraction can be used to target protestors without an appropriate legal framework or safeguards.[15]

For these reasons, PI:

- supports the deletion of **Article 30bis** and **Article 30ter**.

Chapter V – International Cooperation

With regards to **Article 35** (General principles of international cooperation), PI:

- supports the proposal to narrow **Article 35(1)** to provide for international cooperation for the purpose of investigating and prosecuting the crimes recognized in **Articles 6 to 16** of the Convention. This would help create a clear framework for international cooperation, mitigating the risk of the potential misuse of the Convention to justify abuses of human rights, such as freedom expression and association.
- recommends including a requirement of dual criminality in all cases of international cooperation in **Article 35(2)**. The principle of dual criminality mandates that a conduct must be considered a criminal offense in both the requesting and the requested states for an international cooperation request to be valid. It hence provides a layer of protection for individuals, as it reduces the chance of states being able to request cooperation for offenses that are not universally recognized as criminal. By making

[12] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Informals/Coordinators/Group_6.pdf

[13] See https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

[14] The risks that this surveillance technology poses are well illustrated in the case brought by asylum seeking claimants in the UK, which resulted in a High Court ruling in 2022 that the UK government acted unlawfully and breached human rights and data protection laws by operating a secret, blanket policy of seizing, retaining and extracting data from the mobile phones of asylum seekers arriving by small boats, see https://privacyinternational.org/news-analysis/4987/uk-high-court-orders-groundbreaking-redress-thousands-migrants-affected-unlawful

[15] Other countries are reportedly using such capabilities, e.g., Argentina, https://adc.org.ar/informes/quien-revisa-tu-telefono/

dual criminality obligatory, the provision provides more clarity and predictability for State Parties in terms of their legal obligations.

With regards to **Article 36** (Protection of personal data), this **Article** needs to provide State parties to the Convention with clear, precise, unambiguous and effective standards to protect personal data, and to avoid data being processed and transferred to other states in ways that violate the fundamental right to privacy. To achieve that Article 36 needs to be amended to reflect data protection principles derived from existing international human rights law, which have been recognised in the Human Rights Committee General Comment on Article 17 of ICCPR[16] and in the report of the UN High Commissioner for Human Rights on the right to privacy in the digital age[17], as well as in resolutions of the General Assembly and the Human Rights Council on the right to privacy in the digital age.[18] PI notes that the proposal contained in the working document of the coordinator of Group 10 fails to do the above and, instead, provides very generic and vague standards on data protection.[19]

For these reasons, PI:

- Supports the proposal to include 'including international human rights law' in **Article 36(1)**;
- Recommends including in **Article 36(2)** explicit wording to demand that that states parties require that the personal data are processed for compatible purposes, limited to what is relevant for the purposes of the processing, and kept only as long as needed in view of such purposes, that processing is subject to appropriate measures to keep it accurate and secure, that general information about data processing is provided by way of public notice, and that effective oversight and redress is available.

As far as **Article 47** is concerned, PI is alarmed by its current wording as it risks supporting open-ended law enforcement cooperation without detailing the limitations and safeguards required under international human rights law.

For these reasons, PI:

- supports the proposal to amend **Article 47(1)** to limit the scope of this cooperation to the crimes that are the object of this Convention (Articles 6-16);
- recommends the deletion of Article **47(1)(b), 47(1)(c) and 47(1)(f)**, aiming to prevent States Parties from sharing personal data in ways that bypass the safeguards embedded in the Mutual Legal Assistance framework. States should not leverage the Treaty to authorize or require personal information sharing outside the bounds of the existing mutual legal assistance treaty, the safeguards established under the MLA, and the MLA vetting mechanism. Such safeguards should not be removed without providing comparable protections and limitations, and their removal invites misuse of the mutual legal assistance framework for transnational repression. In this respect, we note that under the current proposal, **Article 24** does not apply to the international cooperation chapter, and the current wording of **Article 36** does not specify the minimum data protection principles, therefore the protection afforded to sharing of personal data under this Article is insufficient. Moreover, the data in question has the potential to reveal the location of an asylum seeker or political dissidents, inviting misuse of the criminal mutual legal assistance framework for transnational repression;

[16] UN Human Rights Committee, General Comment No 16: Article 17, UN Doc HRI/GEN/1/Rev.1 at 21 (8 April 1988).
[17] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).
[18] See for example, UN General Assembly resolution on the right to privacy in the digital age, UN Doc A/RES/77/211, para 7(i).
[19] See: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Informals/Coordinators/Group_10_-_Possible_consesus_text_on_Article_36.pdf

- recommends that **Article 47(2)** includes reference to **Article 24** and **Article 36**, as a crucial condition for any law enforcement cooperation must be to ensure respect for privacy and data protection.

As far as **Article 48 bis** (Special investigative technique) is concerned, PI underlines that the undefined term "special investigative techniques" and an open-ended reference to methods "such as electronic or other forms of surveillance" could be interpreted to justify the application of very intrusive surveillance technologies including those that have not yet been developed or that are inherently disproportionate in nature, and therefore prohibited under international human rights law. It may also be used to justify government hacking, which would likely result in violation of the right to privacy as well as compromising the security of digital communications. Government hacking can be far more privacy intrusive than any other surveillance technique, permitting remote and secret access to personal devices and the data stored on them, as well as the ability to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking also allows governments to manipulate data on devices, including corrupting, planting, or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion. It not only poses unique privacy interference to the intended targets, but it often affects the privacy and security of others in unpredictable ways. Hacking is about causing technologies to act in a manner the manufacturer, owner, or user did not intend or did not foresee. In its most dangerous form, government hacking depends on exploiting unpatched system vulnerabilities to facilitate surveillance objectives.[20]

For these reasons, PI:

- recommends that **Article 48bis** is not included in the Convention.

Chapter VII – Technical assistance and information exchange

As far as **Article 54** (Technical assistance and capacity-building) is concerned, PI notes that, in light of recent reports on the misuse of certain surveillance technologies by several states, UN Special Rapporteurs, the High Commissioner for Human Rights and other independent experts have called for the adoption of control regimes applicable to surveillance technologies, including requiring "*transparent human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms.*"[21]

Within the European Union, in November 2021 the European Ombudsperson opened an investigation into how the European Commission assessed the human rights impact before providing support to African countries to develop surveillance capabilities. It concluded that the measures in place were not sufficient to ensure the human rights impact of EUFTA projects was properly assessed.[22] Further, following a series of revelations made by a group of media organisations reporting that NSO Group's Pegasus software was being used against journalists, activists and politicians in numerous countries across the world including in Europe,[23] a European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware was set up. In its final report and recommendation adopted on 8 May 2023, after 14 months of hearings, studies, and fact-finding missions, the Committee underlined that the abuse of surveillance technologies such as spyware "*undermines*

[20] For more details, see PI and EFF''s submission to the fourth session, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf

[21] UN High Commissioner for Human Rights, report on the right to privacy in the digital age, A/HRC/51/17, paragraph 56.

[22] https://www.ombudsman.europa.eu/de/decision/en/163491.

[23] https://www.theguardian.com/news/series/pegasus-project.

democracy and democratic institutions by stealth. It silences opposition and critics, eliminates scrutiny and has a chilling effect on free press and civil society".[24] It therefore called on EU institutions to "*implement more rigorous control mechanisms to ensure that […] the donation of surveillance technology and training in the deployment of surveillance software, does not fund or facilitate tools and activities that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights…*".[25]

PI recommends that:

- **Article 54(1)** includes the following additional wording: "State Parties shall ensure that any technical assistance and capacity building is conditional upon prior human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms."

[24] https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_section2.
[25] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html.