ARTICLE 19's briefing

The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol

In the context of ongoing international negotiations for an international convention on cybercrime, reference has been made to the Council of Europe Convention on Cybercrime (Budapest Convention) as a benchmark for addressing criminal sanctions in cyberspace. While the Convention contains some positive features, including codified intentionality requirements, and avoids many pitfalls that ARTICLE 19 has analysed in various domestic cybercrime instruments (such as lack of intentionality requirements, lack of requirements of "serious harm," and content-based offences), it fails to strike a proper balance for freedom of expression. As such we believe that it is not a model instrument from a human rights perspective. In this briefing, ARTICLE 19 highlights freedom of expression issues with the Budapest Convention and identifies problems that should not be replicated in the text of the new instrument. We hope that this analysis will guide the work of the Ad hoc Committee as it moves to the next stage of the negotiations.

Background to the Budapest Convention

The Council of Europe has been working since 1989 to address threats posed by hacking and other computer-related crimes, and the Council of Europe Cybercrime Convention (the Budapest Convention or Convention) represents the culmination of these efforts. The Convention's drafting controversially excluded civil society. Law enforcement interests dominated the drafting process from the outset, and nineteen drafts were completed before it was released for public comment. The Council of Europe has made little effort to address the concerns of other stakeholders in the process but has provided an explanatory report with more detailed context behind the Convention's provisions.

The Convention entered into force on 1 July 2004 and is presently the most widespread international legal framework addressing criminal sanctions in cyberspace. More than sixty parties have ratified the Convention, including numerous non-Council of Europe States, including but not limited to the United States, Canada, South Africa, Japan, Australia, and Israel. Importantly, many States look to the Convention and its additional protocols as benchmarks for international cyber legislation.

The Convention is divided into four chapters:

- The first chapter contains definitions of computer systems, computer data, service providers, and traffic data.

- The second chapter deals with measures to be taken at the national level, and is divided into two sections:

- The first section deals with substantive law issues: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright.

- The second section deals with procedural and law enforcement issues, including preservation of stored data, preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data and interception of content data.

- The third chapter contains provisions concerning mutual legal assistance and extradition rules.

- The fourth and final chapter contains the final clauses, which deal with standard provisions in Council of Europe treaties.

The key issues from a free speech perspective

Failure to provide specific procedural protections for privacy and freedom of expression

While the Budapest Convention begins in its preamble by stating that it is "mindful" of the "need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights," citing numerous international human rights instruments and the protection of freedom of expression, the integration of human rights standards appears to end there. The Convention fails to address privacy rights and focuses almost completely on providing expansive powers to law enforcement. It fails to provide specific procedural protections for privacy and freedom of expression to appropriately counterbalance the specific and extensive law enforcement powers it mandates.

We note that following feedback from civil society, the Budapest Convention incorporated Article 15, requiring that each party ensure that implementation of the powers and procedures of the Convention "are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality." However, this section does not provide specificity as to what is meant by "conditions and safeguards," and the general vagueness of these protections lies in contrast with the significant privacy-invasive provisions present in the rest of the Convention.

Unnecessary content- and copyright- offences

The first section of Chapter II of the Budapest Convention lays out substantive criminal law offences. Title I requires Parties to criminalise **five** offences against the confidentiality, integrity and availability of computer data and systems.

- **Illegal access.** Article 2 requires Parties to criminalise "Illegal access," which includes the intentional access to whole or part of a computer system without right. A Party may optionally require that the

offence be committed by infringing security measures, with the intent of obtaining computer data or dishonest intent.

- **Illegal interception.** Article 3 requires Parties to criminalise "Illegal interception," which criminalises the intentional interception without right, by technical means, of non-public transmissions of computer data from or within computer systems. Similarly, a Party may require the offence to be committed with dishonest intent.

- **Data interference.** Article 4 requires Parties to criminalize "data interference," or the intentional damaging, deletion, alteration, or suppression of computer data without right. A Party may optionally require that the conduct result in "serious" harm.

- **System interference.** Article 5 requires Parties to criminalise the "serious hindering without right" of the functioning of a computer system by inputting, transmitting, damaging, deleting, or altering computer data.

- **Misuse of devices.** Article 6 requires Parties to criminalise the production, sale, or import of devices, including programs, "designed or adapted primarily for the purpose of committing" any of the aforementioned offences, or of computer passwords or access codes, with "intent" that such items be used for the purpose of committing the aforementioned offences. Article 6 includes a provision protecting from criminal liability the sale, production, import, or distribution of items for "authorized testing or protection of a computer system," such as for research.

ARTICLE 19 observes that, while these offences require intentionally, important substantive protections are merely optional. For instance, the provisions on illegal access and interception do not explicitly require "dishonest intent." Neither does data interference require "serious" harm to occur.

ARTICLE 19 is also gravely concerned that the Budapest Convention does not adequately protect the work of digital security activists working to protect and promote freedom of expression. For instance, the implementation of the Convention in Brazil may leave open the criminalisation of the development of secure digital communications tools by activists. The protection for possession of items for authorised testing does not provide clarity as to justified users of offending devices, as activism and digital rights research may extend beyond the scope of "authorized testing or protection of a computer system."

Title II requires the criminalisation of **two** computer-related offences:

- **Computer-related forgery.** Article 7 requires Parties to criminalise the intentional input, alteration, deletion, or suppression of computer data that results in "inauthentic data" with the intent that it be "considered or acted upon for legal purposes as if it were authentic." Parties may optionally require an "intent to defraud, or similar dishonest intent."

- **Computer-related fraud.** Article 8 requires Parties to criminalise intentionally causing the loss of property to another person by input, alteration, deletion or suppression of computer data, or any interference with a computer system's function, with fraudulent or dishonest intent of procuring, without right, an economic benefit.

Title III requires criminalisation of **one** content-related offence, **child pornography.** Article 9 requires Parties to criminalise the production, distribution, or procurement of child pornography, including "realistic images" representing minors engaged in explicit conduct, with the definition of "minor" including persons under 18 years of age. Parties may require lower age limits of not less than 16 years.

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 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." As 176 States are already parties to the Protocol, which provides for mutual investigative assistance, it is unclear that a cybercrime treaty is a necessary place to impose content-based obligations.

Title IV requires criminalisation of **copyright infringement.** Article 10 requires Parties to criminalise copyright infringement and related rights pursuant to a number of existing international instruments, with Parties able to reserve the right not to impose criminal liability if other remedies are available.

ARTICLE 19 questions the need to include copyright-related criminal offences in a cybercrime measure, as well as the compatibility of criminal sanctions for non-commercial copyright infringement with freedom of expression. Such sanctions have a chilling effect on the free flow of information and are a disproportionate interference with the right to freedom of expression. In *The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age* (2013), we recommend that criminal laws related to copyright infringement at a minimum conform to the following:

- Offences for copyright infringement may only be compatible with the right to freedom of expression and information if they have a clear legal basis, each element of the offence is clearly defined and the range of sentences available is proportionate to the seriousness of the offence.

- There is no public interest in bringing a prosecution in non-commercial copyright infringement cases. Therefore, law enforcement authorities should not initiate such prosecutions

- Prison sentences, suspended prison sentences, excessive fines and other harsh criminal penalties should never be available as a sanction for non-commercial copyright infringement.

We are concerned that no analogous protections apply or are even recommended in the Budapest Convention, thus encouraging Parties to adopt disproportionate restrictions criminalising copyright infringement.

Title V in Articles 11 and 12 provides for the punishment of attempted violations of the aforementioned provisions, or for aiding or abetting, as well as corporate liability. As a result, ARTICLE 19 believes the Convention fails to be balanced and proportional. It fails to define key terms such as "content data," includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no analogous standards to protect privacy and limit government use of such powers.

All in all, while ARTICLE 19 questions the necessity of an international cybercrime instrument, at the maximum only some offences from the Budapest Convention should be considered, name access and interception offences with clear requirements of "serious" harm and "dishonest" intent.

Far-reaching procedural provisions for law enforcement seizure and surveillance powers

Invasive Law Enforcement Techniques

Articles 16 and 17, Expedited Preservation of Stored Computer Data, and Expedited Preservation and Partial Disclosure of Traffic Data, respectively, detail law enforcement practices with significant privacy implications. ARTICLE 19 is concerned that neither of these sections include meaningful limitations on these techniques.

Search and Seizure of Stored Computer Data

Article 19, Search and Seizure of Stored Computer Data, enables investigative authorities to search and seize computer systems or data. This provision does not include accompanying confidentiality protections for materials obtained through production orders. Further, this may contemplate the adoption of laws that can force users to provide encryption keys or plain text of encrypted files.

Section 4 requires laws to empower authorities to "order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information." In 2015, the Special Rapporteur on freedom of expression presented to the General Assembly his report on encryption and anonymity in the digital age. The result of the report was the finding that restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law, as both are essential components for the exercise of freedom of expression online. The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online." The report stipulated that such orders should be i) based on publicly accessible law; ii) clearly limited in scope and focused on a specific target; iii) implemented under independent and impartial judicial authority, in particular, to preserve the due process rights of targets; and iv) only adopted when necessary and when less intrusive means of investigation are not available.

Real-Time Collection and Interception of Traffic *Data*

In contrast to Article 19 which covers stored data (data at rest), Articles 20 and 21, Real-time collection of traffic data and Interception of content data, respectively, require parties to have domestic laws requiring service providers to cooperate in the collection of traffic data and the content of communications. Article 20 mandates laws to allow authorities to "compel a service provider… to collect or record" or "to co-operate and assist" in recording traffic data. Further, this provision allows confidentiality provisions that may prevent service providers from notifying subscribers of such recordings.

Article 21, analogously, mandates laws to allow authorities to "compel a service provider… to collect or record" or "to co-operate and assist" recording of "content data" in real time. This provision is limited to interception of content data for "serious offences," however the term "serious" is nowhere defined in the

Convention and is left to domestic law. Further, there is no clear definition of "content data" that differentiates it from "traffic data."

Without sufficient privacy and due process protections, these provisions threaten human rights. They lack specific guidelines regarding limits of interception and monitoring and fail to define key terms.

Failure to require dual-criminality as a pre-requisite for mutual legal assistance

One of the Convention's primary shortcomings is its failure to consistently require dual criminality as a condition for mutual assistance between countries. Articles 33 and 34, covering mutual assistance regarding the interception of traffic and content data, respectively allow interception to the extent permitted by other treaties and domestic law. They require mutual assistance in the "real-time collection" of data.

A primary issue is as discussed in the context of Article 21, "content data" is not defined. Article 34 requires Internet providers to cooperate with electronic searches and seizures without reimbursement and does not require dual criminality, or for the underlying basis for suspicion to be a crime in the country in question.

Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

On 20 May 2022, the Committee of Ministers adopted Recommendation CM/Rec(2022)16 to Member States on combating hate speech, citing that Member States "should specify and clearly define in their national criminal law which expressions of hate speech are subject to criminal liability" including "racist, xenophobic, sexist and LGBTI-phobic public insults under conditions such as those set out specifically for online insults in the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems." This Protocol to the Convention on Cybercrime entered into force in 2006 and extended the Convention's scope to cover offences of racist or xenophobic propaganda. It requires Parties to adopt measures to render various types of racist conduct via computer systems criminal offences under domestic law when they are "committed intentionally and without right."

The measures to be taken at a national level include:

- Dissemination of racist and xenophobic material via computer systems (Article 3);
- Racist and xenophobic motivated threat (Article 4) and insult (Article 5);
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity (Article 6);
- Aiding and abetting any of the above (Article 7).

Note that these measures are solely concerned with criminal law measures against online hate speech, which does not leave space for civil or non-legal remedies and responses.

For context, ARTICLE 19 notes that Article 20 (2) of the International Covenant on Civil and Political Rights provides that any advocacy of national racial or religious hatred that constitutes incitement to discrimination, hostility or violence is to be prohibited by law. However, it does not call for criminalisation, and States are not obligated to criminalise such expression. The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence ("the Rabat Plan"), is authoritative guidance on interpreting Article 20(2) based on conclusions and recommendations emanating from four regional expert workshops organised by the OHCHR and adopted by experts in Rabat, Morocco, in 2012. The Rabat Plan outlines a six-part threshold test taking into account (1) context, (2) status of the speaker, (3) intent to incite the audience against a target group, (4) content and form of speech, (5) extent of dissemination and (6) likelihood of harm.

In its judgment of 17 July 2018, the European Court of Human Rights referenced the Rabat Plan of Action. In August 2019, the High Commissioner addressed the Security Council in an Arria-formula meeting on advancing the safety and security of persons belonging to religious minorities in armed conflicts. In his 2019 report to the General Assembly, the UN Special Rapporteur on freedom of expression recommended companies adopt content policies that tie their hate speech rules directly to international human rights law, citing the Rabat plan.

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. The primary impetus cited for the Second Additional Protocol is the complexity of obtaining electronic evidence that might be stored in foreign or unknown jurisdictions, thus providing a framework for disclosing domain name registration information and mutual assistance tools. Civil society has urged the drafters to appropriately include civil society and privacy regulators. As a result of its shortcomings and failure to properly protect privacy, the Protocol has faced criticism from the European Data Protection Board.

The final version of the Second Additional Protocol places few limitations on the power of law enforcement to collect data, which has negative implications for journalists, activists, and the rights of privacy and freedom of expression online. The Protocol fails to recognise the importance of anonymity online. Further, it does not require proper safeguards for police powers. Article 7, for instance, which is the main vehicle for cross-border obtaining of subscriber data, requires Parties to eliminate legal obstacles for "direct cooperation" between companies and law enforcement, effectively writing legal safeguards out of the picture. Article 14 provides some limited data protection obligations, but these protections can be removed by mutual agreement between two signatories. Further, Article 14 does not require independent oversight of law enforcement and prohibits additional safeguards in the use of biometric information. The net effect of this is to impose international law enforcement powers while failing to correspondingly apply human rights protections.

Finally, the Second Additional Protocol falls short of the Council of Europe's data protection regime in Convention 108+, and aspects of the approach to subscriber data contradict case law of the European Court of Human Rights.

For the aforementioned reasons, ARTICLE 19 recommends caution in directly implementing the framework of the Budapest Convention, which does not inherently strike an appropriate balance between fundamental rights and the prevention of cybercrime online. Repeating the same flaws of the Convention and its Additional Protocols threatens to undermine the protection of privacy, the applicability of international and regional instruments, and the availability of judicial review.