Submission by Human Rights Watch to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes
April 2022

Introduction

Human Rights Watch is an independent, nongovernmental organization that monitors and reports on human rights in around 100 countries around the world. Human Rights Watch also conducts extensive research and advocacy on thematic issues, including technology and human rights. For over a decade, Human Rights Watch has reported on risks to freedom of expression, association, assembly, and privacy posed by national legislation and international cooperation to address cybercrime.

Countering cybercrime is a timely and pressing challenge but should not come at the expense of the fundamental rights and dignity of those whose lives this proposed treaty will touch. Human Rights Watch is not convinced a global cybercrime treaty is necessary and is concerned that it risks eroding human rights protections and States' obligations under international rights law. Nonetheless, Human Rights Watch welcomes the opportunity to provide input to the work of the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Preamble and General Provisions

Cybercrime poses a real threat to people's human rights and livelihoods and efforts to address it need to protect, not undermine, rights. The preamble and general provisions, and the proposed treaty as a whole, should be consistent with States' human rights obligations set forth in the

Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Convention on the Elimination of All Forms of Racial Discrimination (CERD), the Convention on the Rights of the Child (CRC), and other international and regional human rights instruments and standards.

These negotiations should not seek to reinvent or redefine human rights standards, such as what constitute permissible restrictions on freedom of expression, limitations on the right to privacy, due process standards or other relevant rights. Rather, the proposed convention should reinforce States' obligations under international human rights law to protect people from harm resulting from criminal activity carried out through the internet while respecting other international human rights standards.

Criminalization

Governments have obligations under international human rights law to protect people from harm resulting from criminal activity carried out through the internet. But government responses to cybercrime are often ineffective or disproportionate and can undermine rights. From a human rights perspective it is essential to ensure any potential treaty defines offenses in precise terms that do not threaten or undermine rights and to keep the scope of offenses narrow to focus on core cybercrimes.

Human Rights Watch's reporting has documented the use and consequences of vaguely worded or overbroad cybercrime laws to crack down on freedom of expression and association, including to censor online content, block websites, or even entire platforms.

For instance, some governments are putting into place cybercrime laws with provisions that directly violate freedom of expression, by criminalizing anyone who "prepares or disseminates" information through any information system or device with the intent to praise a person "accused of a crime," or to "advance religious, ethnic or sectarian hatred," or with intent to praise terrorism or proscribed organizations. Other governments are adopting cybercrime laws that purport to protect national security, public order, or public health or morals, but do so in such overbroad and vague ways that they lend themselves to crackdowns on freedom of expression. Other trends include disproportionate measures, like the criminalization of defamation online, which puts at risk anyone who questions the government or other state institutions.

Many countries have made spreading "false" information or rumors online a cybercrime. What is "false" is often highly contested, and criminalizing "false" statements opens the door to broad criminalization and chilling of speech. Human rights experts at the UN and regional bodies have

long condemned governments for using vague and ambiguous terms such as "false news" and "non-objective information" to outlaw disseminating certain types of information.

International human rights law requires any regulation of freedom of expression to be necessary for a legitimate purpose, and proportionate to that end. Even when a law has a legitimate purpose, governments are obligated to specifically identify the nature of the threat being addressed and how the measure proposed is both a necessary and proportionate means of addressing it.

Cybercrime laws are often wielded against people who are marginalized or vulnerable in society because of who they are, what they believe, or their advocacy for human rights. For example, such laws are used to persecute and imprison bloggers, journalists, human rights defenders, activists, political opponents, and free thinkers. So-called morality clauses have led to arrests and prosecutions of women and LGBT people for expressing themselves online. A new treaty risks legitimizing and normalizing these practices. The provisions of any potential cybercrime treaty should not lend themselves to interpretations that improperly restrict conduct protected under international human rights standards.

Both the spread of disinformation that undermines human rights and online gender-based violence require a government response. However, government responses to these human rights challenges that focus on criminalization of content can also lead to disproportionate restrictions on rights, in particular the right to freedom of expression and privacy.

International human rights frameworks provide guidance with respect to online gender-based violence in particular. For example, the Committee on the Elimination of Discrimination against Women's General Recommendation 35 provides authoritative guidance on States' obligations to eliminate gender-based violence against women, which it defines to include "contemporary forms of violence occurring online and in other digital environments." General Recommendation 35 advises States Parties take a range of actions, including general legislative measures, preventative measures, protective measures, prosecution and punishment measures, provide for reparations for victims/survivors, coordination, monitoring and data collection, and international cooperation. Focusing on creating content-related offenses in the proposed cybercrime treaty creates serious human rights risks, without addressing the need for a more holistic and effective response to the problem. States concerned about the proliferation of online gender-based violence should work to advance implementation of international human rights treaties like CEDAW, including by fulfilling their existing obligations to eliminate online gender-based violence through the required domestic measures.

The criminalization chapter of the proposed convention should focus on core cybercrimes. Just because technology might be used in the commission of a crime does not make it a "cybercrime"

and therefore within the scope of the proposed convention. Articles 2-6 of the Budapest Convention provide useful guidance for the scope of the proposed treaty. These include illegal access to computing systems, illegal interception of communications, data interference, system interference, and misuse of devices.

Even a narrowly tailored treaty that criminalizes core cybercrimes can be misused or abused to violate rights, which is why the potential treaty should include human rights safeguards that apply to the criminalization provisions as well as procedural ones. For example, whistleblowers and journalists can face prosecution for having "unauthorized" access to systems and data to expose government or corporate wrongdoing. A clearly articulated and expansive public interest defense and a malicious intent standard are needed to protect against the criminalization of whistleblowing and journalistic activity. Moreover, core crimes need to define access "without authorization" narrowly, to exclude legitimate activities such as those by security researchers and journalists.

It is also of crucial importance that the treaty not criminalize encryption or anonymity online. Strong encryption is critical to protecting human rights and cybersecurity in the digital age, both for ordinary people, as well as for journalists and human rights defenders. End to end encrypted communications platforms and any tools that use encryption protocols should be effective and robust, without built-in vulnerabilities, often called "backdoors," that can be exploited by abusive actors.

Procedural Measures and Law Enforcement

Police around the world are using an increasingly intrusive set of legal and technical arrangements, as well as surreptitious measures, to access digital evidence, which can include people's personal data. Direct and unrestricted access to communications data constitutes a serious interference with the right to privacy. Obtaining target-based data from internet service providers and other online services such as social media platforms or cloud storage services can be essential for investigating and prosecuting cybercrime. However, some legal and technical arrangements, as well as measures that fall outside the rule of law, can lead to the disproportionate collection and retention of data, without judicial oversight and basic due process protections.

This is particularly the case when law enforcement compels companies to grant unrestricted access to subscriber data, traffic data, and even content data in real time. Such obligations are often paired with harsh sanctions on companies for failure to retain data and provide access to law enforcement. Frequently, their investigations cross borders without proper safeguards and bypass the protections in mutual legal assistance treaties.

It is crucial that the procedural measures and law enforcement provisions of the proposed convention ensure that any interference with the right to privacy, including through the collection of metadata, complies with international human rights standards, namely, principles of legality, necessity, and proportionality. That should include by requiring independent and competent judicial authorization of surveillance measures that intrude on privacy, meaningful oversight of surveillance measures, and respect for due process rights.

Requirements that force companies to grant authorities unrestricted access to systems or massive amounts of information collected and stored by private actors constitute a serious interference with the right to privacy and should be excluded from the potential treaty. They are particularly prone to abuse, circumvent key procedural safeguards, and exceed the limits of what can be considered necessary and proportionate.

It is crucial that the same safeguards outlined above apply when authorities seek access to cross-border digital evidence. These safeguards should cover all persons found under the control or jurisdiction of the State irrespective of their nationality or other distinctive characteristic.