The UN Cybercrime Convention: why it endangers human rights defenders and journalists

Sara Benitez - Mongelos*

Abstract: The UN Convention on Cybercrime was adopted in spite of multiple concerns regarding the unlimited prosecution powers it grants states. In Latin America, where human rights defenders and journalists are constantly harassed and threatened, this Convention could add to their vulnerability.

The United Nations Convention against Cybercrime was adopted by the UN General Assembly on December 24, 2024, by resolution 79/243. As the first comprehensive global treaty on cybercrime, it outlines measures for states to prevent and combat cyber-related offenses. Additionally, it seeks to enhance international cooperation in the exchange of electronic evidence for serious crimes. Comprising nine chapters, this Convention offers a thorough framework for addressing cybercrime while incorporating safeguards for human rights. It addresses technical and legal challenges by adapting traditional investigative methods to the digital landscape and reinforcing international collaboration.

*Sara Benítez-Mongelós is a Paraguayan lawyer, public translator, researcher, and University lecturer. She has a Master's in Human Rights and Democracy in Latin America and the Caribbean (LATMA) from the Global Campus Latin America in Buenos Aires (Cohort 2022-2023). Currently, she is in the process of publishing her research on disappearances perpetrated by non-state actors in Paraguay.

Regarding the status of this Convention, it will be open for signature at a formal signing ceremony to be held in Hanoi, Vietnam, in 2025. Following this event, it will remain available for signature at the United Nations Headquarters in New York until December 31, 2026. This treaty will enter into force once the fortieth instrument of ratification, acceptance, approval, or accession has been deposited.
A relevant question arises as to whether the adopted Convention against Cybercrime endanger human rights defenders and journalists. The unanimous answer amongst scholars, activists, and civil society organisations seems to be yes.
While the new Convention aims to address the pressing issue of cybercrime, the present post does not seek to diminish its efforts toward positive change, but to examine certain aspects of the treaty that may raise concerns for human rights activists and defenders. Rather than enhancing their protection, some provisions could inadvertently increase their vulnerability. This analysis is intended as a form of constructive criticism, offering an academic perspective to contribute to the broader discourse on the Convention's implications.

First, states are granted excessive powers to collect sensitive and private/personal data without the obligation to comply with the principles of proportionality, necessity and legality, with no human rights safeguards that tackle all these security concerns. This can lead to gross human rights violations of every individual, but even more so, of those who are on the frontlines defending human rights and denouncing acts of corruption and illegality in their governments, such as journalists and activists.
While making cyberspace a safer place is a valid argument, the Convention against Cybercrime increases the number of tools that states have in order to pursue and combat illicit online activities, through the classification of different crimes and the establishment of international cooperation and technical assistance. However, it falls short on the guarantees it provides for individuals, especially for women and LGBTQIA+ who work as journalists and activists.

Second, the Convention against Cybercrime does not take into consideration the protection of vulnerable individuals, and in fact, it endangers them, because this treaty could be used by authoritative governments as a tool to criminalise human rights activists and journalists when they take their claims to the online space, such as denouncing government officials through their social media, which could be rated by the government as cybercrimes. This Convention can set the tone for countries that are still developing their cybercrime legislation, or it can be used by other countries that already have concerning existing cybercrime laws to legitimise the persecution of human rights defenders, activists, and journalists.

Third, the new Convention does not include a gender- based perspective or gender-based standards in its provisions. According to the report by *Derechos Digitales*:

> Cybercrime laws normally refer to non-gender-specific acts or are designed without due consideration to gender inequalities. Criminal definitions are drafted in a broad manner and without applying a gender perspective in their formulation and in their implementation. As a result, the impact of the criminalisation generated by these laws also has specific effects on gender equality.

Cyberspace is inherently a more hostile environment for women than men, and for that reason, it is imperative to incorporate the gender perspective into the text of the Convention and the successive protocols that will ensure its entry into force.

Fourth, the scope of the definitions of terms and wording of the new treaty is too broad and extends far beyond those situations where the use of digital technologies is essential to the commission of a crime. Most of them relate to the punishment of different forms of speech, making them susceptible to censorship and political persecution. This is extremely dangerous, especially in countries with fragile democratic institutions or under an authoritarian regime. Consequently, there is a lack of adequate human rights safeguards to prevent the treaty from enabling oppression by means of potential censorship and political persecution to those who dissent with the government.

Fifth, in regard to state cooperation, there are no safeguards regarding cross-border data collection and sharing of information between states: there is no set of minimum requirements to guarantee fundamental rights. Without the observance of human rights standards, these provisions could allow states to collect and share personal information on citizens with each other, without adequate safeguards to prevent governmental abuse of power. This could include, for example, revealing personal identities, applying domestic laws to acts that are contrary to international human rights law but legal in domestic law (for instance, punishment for showing solidarity with or being part of the LGBTQIA+ community), criticising the government, protesting, marching, being vocal on social media about government wrongdoings. In some cases, this could also be used against investigative reporters, who through their work, expose and denounce government corruption. This could allow governments to invade cyberspace and gain access to journalists' personal information, work and their sources and share it with other states.

In summary, the Convention against Cybercrime favours extensive surveillance, establishes weak privacy safeguards, and defers most protections against surveillance to national laws, which is dangerous, especially in those with weak institutionality, authoritative governments, high levels of corruption and with reputations of not complying with international human rights law and its standards.

Recommendations

To ensure that the implementation of the Convention will effectively protect human rights once it will enter into force, it is crucial to incorporate stronger safeguards for online security, particularly for individuals at risk due to their work defending and promoting human rights, such as activists, human rights defenders, and journalists. This Convention should explicitly include an effective, intersectional gender perspective and guarantee special protection for vulnerable groups, including the LGBTQIA+ community.

Additionally, under the same Convention clear limitations on state powers should be established regarding the collection and use of personal and private information. Safeguards must prevent the misuse of such data to target individuals engaging in legitimate activities—both online and offline—related to promoting accountability, transparency, and good governance.

Furthermore, the ability of states to gather, process, and share citizens' personal information with other states should be subject to strict oversight. This is essential to prevent potential abuses, including unjust prosecution, censorship, or persecution of human rights defenders investigating cross-border issues that may expose governmental misconduct.

Therefore, the Convention against Cybercrime could be strengthened through annexes providing additional guidelines and mechanisms for safeguarding human rights. These annexes could detail specific obligations upon states regarding digital security, privacy protections, and accountability measures, ensuring the treaty remains a robust tool for the defence of fundamental freedoms while preventing state overreach.