The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy

Katitza Rodriguez ⋮ 16-20 minutes ⋮ 8/27/2024

The United Nations Convention on Cybercrime, even before negotiations began, raised significant alarm within the global human rights community. These concerns escalated further when, on August 8th, UN Member States unanimously adopted the convention, following unsuccessful last-minute efforts to remove central human rights protections.

The Convention defines a series of specific crimes, including attacks on computer systems and cyber-enabled offenses relating to child sexual abuse material (CSAM), outlines intrusive domestic surveillance powers, and authorizes cross-border cooperation in relation for any serious crime—defined as offenses punishable by at least four years of imprisonment, with the specific crimes determined by each country's domestic law, including those offenses that have no nexus to cybercrime or technology at all.

The Convention, hailed as a "landmark step as the first multilateral anti-crime treaty in over 20 years," has rightfully sparked widespread concern for a diverse coalition of human rights organizations, press freedom organizations, the Office of the High Commissioner on Human Rights, the UN rapporteur on protecting human rights while countering terror, major tech companies, industry groups, and leading security researchers.

Many have warned that the treaty is vulnerable to misuse, with significant implications for human rights. The treaty's safeguards are general and, in key provisions, defer to national laws which are too often inadequate. It also lacks mechanisms to monitor compliance with international human rights standards. These weaknesses create a high likelihood that the powerful global cooperation tools the treaty creates will be abused.

In terms of next steps, it is anticipated that the Convention will be adopted by the UN General Assembly at some point this year. After adoption, the treaty becomes open to signature by countries and enters into force 90 days after the 40th country ratifies, accepts, approves or accedes to it. For some states, this process will require parliamentary approval.

It is important for states to carefully consider the human rights implications of adopting this Convention and, should they adopt it nonetheless, to ensure that adoption is accompanied by heightened, detailed safeguards to minimize the convention's most harmful elements.

Key Human Rights Concerns

Core Human Rights Clause Without Specific Safeguards

Article 6.2 states generally that "nothing in this Convention shall be interpreted as permitting the suppression of human rights or fundamental freedoms." Article 6.2 is designed to prevent the treaty from explicitly authorizing use of the convention's powers and provisions to suppress human rights, especially among states that have not adopted relevant human rights treaties. This is an important safeguard to include in principle, and any State party attempting to invoke the treaty to suppress rights like freedom of expression, religion, or association would be acting contrary to this provision.

However, the treaty fails to adopt specific safeguards necessary to truly protect human rights. Indeed, a number of states continue to argue that this provision provides significant deference for national preferences and sovereignty, with one state even arguing that Article 6.2 imposes no obligations on states that have not separately adopted a human rights treaty. States that are already the least human rights-observant are thus already poised to misuse the treaty to suppress further human rights.

Optional and Inadequate Human Rights Safeguards for Intrusive Surveillance

Article 24 of the treaty addresses conditions and safeguards relating to the Convention's chapter on "Procedural measures and law enforcement," but ultimately falls short by allowing significant deference to domestic law, over international standards, in how they are applied. While Article 24.1 mandates that surveillance powers respect human rights safeguards and proportionality, it lacks explicit requirements for the core human rights principles of legality, necessity, and non-discrimination.

Article 24.2 likewise adopts a number of safeguards including the need for judicial review and the need for grounds justifying the use of an investigative power, but leaves them as potentially discretionary and contingent on domestic law. That is highly problematic because many national laws do not meet international human rights standards. For example, many states fail to require prior judicial authorization on the basis of reasonable suspicion for intrusive surveillance powers such as interception of communication or real time collection of traffic data, among others. Article 24.2 also fails to explicitly include key human rights safeguards such as the right to individual notification, opening the door to gag orders and abusive covert surveillance with impunity. Instead of creating global investigative cooperation on the basis of robust human rights safeguards, the treaty seeks to accommodate the worst surveillance practices.

Perpetuating a Culture of Secrecy

The treaty undervalues transparency and undermines due process by imposing strict secrecy requirements. This confidentiality can lead to unchecked power, undermine transparency, and prevent individuals from knowing they are under surveillance and from challenging such actions. By embedding a confidentiality-by-default paradigm and failing to require the well-established human rights obligation to notify impacted individuals of covert surveillance practices to the degree possible, the convention embraces an approach where surveillance abuses can occur with impunity.

For example, the treaty obliges custodians of data, service providers and, in the context of cross-border requests, even governments to keep the use of various surveillance powers confidential (e.g., Articles 29.3 and 40.20). Some provisions even explicitly allow states to require, as appropriate, that there be "no notification to the user" (Article 42.3.g). Confidentiality is broadly mandated, subject only to some narrowly defined exceptions. Some service provider gag orders should include time limits, but the duration of these limits is left to the discretion of national law (Article 25.4). States are permitted to disclose information received under a gag order from other states in proceedings to the degree the information is considered exculpatory in their legal system (Article 40.5) or if some other element of their national legal system compels them to do so (Article 40.20).

Cross-Border Data Sharing Without Sufficient Safeguards

The treaty's international cooperation chapter compels countries to collect and share private data across borders, effectively requiring them to assist each other in electronic surveillance for a wide range of "serious" crimes, whether or not technology is involved in the crime. The cross-border evidence gathering applies to any crime that a state chooses to punish with at least four years of imprisonment under its national law, subject to certain restrictions. Proposals to define "serious crimes" in line with human rights law as crimes that threaten bodily harm or significant financial interests were not adopted, meaning that states might apply the label without any consideration of proportionality and decide for themselves what crimes qualify for global cooperation.

While Article 24 imposes some limited conditions and safeguards on surveillance powers, its application is limited. Specifically, Article 24 only applies if a state is using a power covered by Chapter IV (Procedural Measures and Law Enforcement) when responding to a request under Chapter V (International Cooperation). This means that much of the cross-border evidence sharing contemplated by the Convention is authorized without any meaningful conditions and safeguards at all. As a result, the treaty may allow—and even require—cross-border sharing of evidence obtained through methods that could be considered abusive or highly intrusive.

For example, blanket generalized data retention is problematic under human rights law but states that ignore these restrictions can respond to assistance requests by sharing evidence that was retained through blanket data retention regimes. Encryption is also protected under international human rights

standards but nothing in this convention prevents a state from employing encryption-breaking powers when responding to a cross-border request to access data.

Authorizing Predictive Policing and Biometric Databases

Article 47.1.c on law enforcement cooperation authorizes problematic predictive policing systems and open-ended sharing of sensitive biometric information. Article 47.1.c mandates close cooperation between State Parties' law enforcement agencies, particularly in sharing "necessary items or data for analytical or investigative purposes." While this power is limited to crimes included in the convention, the article is alarmingly vague, and does not tie use of evidence to specific criminal investigations or proceedings. This opens the door to a host of problematic and algorithmically-driven predictive policing applications.

Negotiators considered proposals for more robust data protection standards that would have prevented police from reusing evidence for generalized analytical systems like predictive policing models. Predictive policing tools and biometric databases are highly intrusive, prone to replicating discriminatory bias, and are disproportionately used to target marginalized communities, further entrenching systemic human rights violations. But protections on the use of these tools did not make it into the final draft. There's also no exclusion for sharing personal data, including highly sensitive biometric, traffic, and location data.

Moreover, Article 47.1.c paves the way to sharing of sensitive biometric data and even risks the creation of international DNA or facial recognition evidentiary databases. As noted above, core checks and balances such as the need for proportionality in Article 24 do not apply to international cooperation provisions such as Article 47. The convention also excludes the human rights obligation to provide heightened safeguards for sensitive biometric data and, in fact, fails to include any meaningful data protection requirements, deferring instead to national law (Article 36).

Expanding Mutual Legal Assistance with Countries with Poor Human Rights Records

The Convention undermines human rights by creating a framework for requiring legal assistance between countries that do not already have mutual legal assistance treaties (MLATs) or other cooperation agreements. This framework includes countries that have previously been hindered in their attempts to engage in cross-border surveillance, data sharing and extradition due to their human rights records. There is no explicit mechanism within the treaty for excluding countries that systematically fail to respect human rights or the rule of law from Chapter V, international cooperation mechanisms. The new treaty powers can thus be used to expand the reach of repression on the pretext of fighting crime.

States are still allowed to assess surveillance and data access requests for human rights abuses on a case-by-case basis, but the already overloaded MLAT assessment mechanisms—rightly criticized as slow and inefficient—and the broad scope of cooperation powers for any serious crime risk allowing abusive assistance requests to slip through the cracks while also further delaying the handling of real cybercrime cases.

Lack of Mandatory Grounds of Refusal and Dual Criminality

The Convention excludes requests intended to prosecute or punish someone on the basis of their demographic or related characteristics or political opinions from the scope of international cooperation (Articles 40.22 and 37.15). It also allows states to refuse cross-border data requests on various discretionary grounds, like protecting sovereignty or public order (Article 40.21). Article 40.8 further allows states to require dual criminality as a pre-condition, meaning that states can refuse assistance if the conduct in question is not considered a crime under their own laws. However, nothing in the convention obligates states to actively assess data requests for human rights abuses and many of the grounds for refusal are optional.

The optional nature of dual criminality is particularly concerning, as countries are not required to reject cooperation in investigations for actions that are legal in their own jurisdiction but criminalized elsewhere. This risk is heightened for content-related offenses or other crimes where legal standards vary widely between countries, and where geopolitical interests may influence decisions to cooperate.

Negotiators' proposals to include political offenses—distinct from political opinions—as a basis for refusal were rejected, further weakening the treaty's ability to protect against politically motivated abuses. Exclusion of political offenses is a common safeguard in cross-border cooperation agreements.

Additionally, Articles 6.2 and 40.22 nominally remove from the scope of the convention any requests for cross-border data-sharing that suppress human rights or is intended to punish someone on the basis of their political opinions or personal characteristics. However, these provisions lack the enforceable measures needed to prevent abuse. For example, this framework theoretically excludes cooperation that aims to criminalize political dissent or LGBTQ+ rights. But Article 40.22 requires "substantial grounds"—a high evidentiary standard—before its exclusion of repressive international cooperation requests can be invoked.

Elements of the Convention Could Undermine Cybersecurity Efforts

Negotiators ignored security researchers' pleas to require malicious or fraudulent intent in core offences, and ensure that studying and exposing security flaws in systems isn't a cybercrime. This isn't a theoretical concern: Researchers around the world are routinely threatened or prosecuted for merely exposing security breaches in order to get them fixed. Likewise neglected were demands to clarify Article 28.4 (compelled technical assistance) that could conscript individual tech employees to provide information regarding security weaknesses, threatening encryption and other security measures for the purpose of assisting governments in surveillance activities.

Ongoing Risks of Expanding the Treaty's Criminal Offenses

While the most problematic proposed criminal offenses in the treaty were ultimately excluded from the Convention, a draft resolution tied to the Convention requires the Ad Hoc Committee to begin negotiating a supplementary protocol that would include additional criminal offenses (paragraph 5). Aside from not being 'cyber crimes', many of the offenses that have been proposed over the course of negotiations (e.g., drug and terrorism offenses) lack any universal definition while others (e.g., blasphemy) are wholly inconsistent with human rights. The concern is that these additional crimes will raise a heightened threat that conduct protected by human rights standards, including free expression and peaceful assembly, will be criminalized.

Only 60 states (less than one third of UN 193 Member States) will need to join the Convention's Conference of State Parties before the protocol can be finalized and adopted, while its drafting and negotiation is set to begin even sooner–no later than two years after the Convention is opened for ratification. Given this expedited timeline and low adoption threshold, the protocol could be adopted before many states even have an opportunity to join. It would also be prudent to assess the Convention in practice – including the insufficiency of its protections in practice—before negotiating on expanding its scope.

***

The UN Convention on Cybercrime, while presented as a global milestone, dangerously weakens human rights by offering broad criminal offense definitions and expansive surveillance powers, both domestically and across borders, with inadequate or at times non-existent human rights safeguards. These flaws open the door to widespread abuse, allowing governments to misuse the treaty for repressive purposes. To protect global privacy, freedom of expression, and human rights more broadly, this treaty must be firmly rejected.

Filed under:

Cyber, cybercrime, Digital Surveillance, European Union, Human Rights, Law enforcement, Mutual Legal Assistance Treaty (MLAT), Surveillance, Technology, transnational repression, United Nations, United Nations General Assembly