Privacy International's statement to the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, March 2022

Item 3 - General Debate

[check against delivery]

Privacy International welcomes the opportunity to participate to the first session of the Ad Hoc Committee.

Privacy International 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. In 2021 the UN General Assembly expressed grave concerns that cybercrime legislation was being misused to target human rights defenders or hinder their work and endanger their safety in a manner contrary to international law. This follows years of reporting from UN independent human rights experts and non-governmental organizations on the human rights abuses stemming from overbroad cybercrime laws.

That is why Privacy International calls for any proposed treaty to include human rights safeguards applicable to both its substantive and procedural provisions.

Privacy International would like to address two main issues, which are contained in a joint letter civil society organisations and experts sent to the chairperson of the ad-hoc committee in December last year.[1]

Firstly, with regards to the scope of the proposed treaty, it is essential to keep the scope narrow to avoid becoming an instrument that justifies states' violations of human rights.

Vaguely worded cybercrime laws purporting to combat misinformation and online support for or glorification of terrorism and violent extremism, can be and have been misused to violate freedom of expression, and to target dissent.

[1] Available here: https://www.privacyinternational.org/advocacy/4739/un-must-include-human-rights-safeguards-proposed-un-cybercrime-treaty

Even laws that focus more narrowly on core cyber crimes are used to undermine rights, targeting digital security researchers, whistleblowers, activists, and journalists.

For these reasons, any future treaty should explicitly include a malicious intent standard and should provide a clearly articulated and expansive public interest defense, as well as include clear provisions that allow security researchers to do their work without fear of prosecution.

Secondly, with regards to safeguards. Privacy International is concerned that investigations into cybercrime is often carried out in a vacuum of guarantees against abuses. In particular, national laws, including cybercrime legislation, are often inadequate to protect against unlawful surveillance and they do not provide for mechanisms of judicial authorisation and effective oversight.

Any potential treaty should detail robust procedural and human rights safeguards that govern criminal investigations pursued under such a convention. It should ensure that any interference with the right to privacy complies with the principles of legality, necessity, and proportionality, including by requiring independent judicial authorization of surveillance measures. Further the role of independent oversight mechanisms, including data protection authorities, should be recognised.

As for cross-border exchange of information pertaining to criminal investigations into cybercrime, mutual legal assistance provisions need to incorporate safeguards, including mechanisms to evaluate whether sharing the information complies with human rights standards.

In conclusion, Privacy International reiterates its recommendation that countering cybercrime should not come at the expense of human rights and that member states should ensure that any proposed cybercrime convention is in line with their human rights obligations.