Privacy International's statement at the concluding session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, 5 February 2024

[check against delivery]

Privacy International welcome the opportunity to intervene at this session.

While we recognise that cybercrimes can pose a threat to the enjoyment of human rights, my organisation has long documented the human rights violations committed under the guise of combating cybercrime. We have also consistently recommended that the UN cybercrime treaty should be narrow in scope and should contain robust safeguards to mitigate the risks of these violations.

Regrettably, the latest draft fails to address many of our significant concerns.

I would like to address three of these concerns.

Firstly, the scope of application of the investigative powers is very broad. Indeed, there is a disconnect between the chapter on criminalisation and the scope of the procedural measures. Under the current text, powers afforded to law enforcement agencies apply to the investigation of criminal offenses committed by means of a computer system as well as the collection of evidence in electronic form of any criminal offense (Article 23.2).

Consequently, the scope of application of Chapter IV appears to be expanded well beyond cyber-dependent crimes. Arguably it would make the treaty one of the most far-reaching in criminal matters. This overbroad scope gives rise to the danger that the Convention will be used to justify the prosecution of the legitimate exercise of human rights.

Secondly, we believe the draft text is unbalanced. It gives sweeping, privacy-invasive powers to law enforcement agencies without robust human rights limitations and safeguards.

For example, the provision on search and seizure of information in paragraph 4 of Article 28 is worded in a way that could open the door to measures to undermine encryption, thereby compromising privacy and security of digital communications.

Also Articles 29 and 30 provide for real-time collection of traffic data and interception of content data. These are extremely intrusive measures that require a set of stringent limitations and safeguards.

Unfortunately, Article 24 does not include some key safeguards well established under international human rights law, such as the principles of legality and necessity; prior independent (preferably judicial) authorization of surveillance measures; and the right to an effective remedy. Further, it leaves too wide discretion on states parties in the scope of application of the human rights safeguards.

Thirdly, the chapter of international cooperation is also very broad in scope of application, and with no detailed human rights safeguards.

For example, in relation to sharing of personal data, the wording of Article 36 fails to provide effective protection, particularly across jurisdictions that do not adequately regulate the processing of personal data in their national laws.

Privacy International joined over 100 civil society organisations and experts to recommend that the Convention should move forward **only** if it pursues a specific goal of combating cybercrime without endangering human rights nor undermining efforts to improve cybersecurity.

The present draft falls far short of this goal and Privacy International recommend to comprehensively revise it or to reject it.

Many thanks.