NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Third Intersessional Consultation
3-4 November 2022

First panel:
A Balancing Act: Human Rights Considerations in the Drafting of the Chapters on General Provisions, Criminalization and Procedural Measures and Law Enforcement of the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Statement of the Office of the United Nations High Commissioner for Human Rights

I would like to thank you, Madame Chair, for the invitation to speak here today.
It is heartening to see that human rights considerations are playing such an important role in the negotiation process, consistently being raised by numerous States and other stakeholders – indeed, combatting cybercrime, and crime in general, in a sustainable way needs to be solidly grounded in human rights.

We all know that cybercrime endangers human rights in many ways, already affecting millions of people. At the same time, criminal law and the associated measures that authorities can take to enforce the law, constitute very significant interferences with the rights of the people targeted. The law needs to be carefully drafted, in compliance with fundamental principles of legality, legitimate aim and necessity and proportionality. As noted in OHCHR's submission to the Ad Hoc Committee of 17 January 2022, national cybercrime laws, including procedural laws, are frequently drafted in an overly broad fashion and used to silence political opponents, oppress peaceful protests, prosecute human rights defenders and hamper the work of journalists. It is, therefore, necessary to ensure that any future international instrument on cybercrime cannot be interpreted to justify such steps.

How can this be done?

In the months since the elaboration process of a new cybercrime treaty began, several proposals have been brought forward. This includes proposals for general human rights clauses. Our Office fully supports the inclusion of general provisions on human rights. They would be very important elements, and could guide interpretation, implementation and application of the treaty. Thereby, they would help align counter-cybercrime measures with human rights. Art. 15 of the Budapest Convention provides an example but is limited to procedural law. We would recommend a broader approach to ensure that commitments to human rights duties apply to all commitments under the new treaty, including regarding criminalisation, procedural measures, and international cooperation. References to specific human rights conventions and rights, such as the right to privacy and the right to freedom of expression, can be useful to strengthen those

clauses but should not be drafted in a way that would exclude any other applicable human rights treaties.

However, such general clauses are not enough. They cannot replace what is the most important contribution to making a future treaty human rights-compliant: well-drafted, precisely targeted specific provisions on criminalization, procedural and investigative measures and international cooperation. The interferences with human rights, such as the rights to privacy, to freedom of expression and to liberty, that are set out in such provisions should themselves be necessary and proportionate to achieve a legitimate aim – even if some interpretative space needs to be left to give States Parties sufficient flexibility to integrate the provisions into their domestic law.

Overly broad or vague provisions in these areas risk fragmentation of laws around the world, contradicting the goals of the future treaty to achieve a level of harmonization. Moreover, as experience has shown, if treaty provisions are not precisely drafted, in line with human rights requirements, it opens the door for an implementation into national law that goes beyond what's acceptable from a human rights perspective. If not done with full consideration of human rights obligations of the States, treaty provisions could even be drafted in a way that seem to compel States to take measures that would conflict with their duties under human rights law. Merely relying on general clauses would in those cases be a weak defence.

It is crucial that every provision of a future treaty should be drafted in full alignment with human rights law, in a way that minimizes their potential for becoming a basis for human rights violations and abuses. This is a main reason for our recommendation that the treaty should focus on core cybercrimes and exclude content-related crimes from its scope. As noted before, cybercrime laws have been and are being used to impose overly broad restrictions on free expression. Provisions prohibiting forms of hate speech and disinformation (to use these broad umbrella terms), for example, are often used to clamp down on criticism of governments, to arrest, harass, prosecute and convict people for merely expressing their political views or religious beliefs. This is not a merely theoretical possibility but a sad reality we observe week in week out.

To ensure that human rights are effectively baked into the treaty, utmost care needs to be taken when shaping the procedural measures that States would be allowed or even required to take. As OHCHR reports have highlighted, surveillance measures that are incompatible with international human rights law are already widespread, eschewing fundamental principles of human rights law. A new treaty should not become a vehicle to continue this trend. Rather, we urge States to seize this opportunity to put down essential requirements and safeguards for the investigative measures needed to fight cybercrime. The treaty should make those requirements and safeguards mandatory and not leave it entirely to the States to decide what they deem appropriate. If this could be achieved, it would be a big step forward towards safeguarding human rights.

As we and others have repeatedly highlighted, procedural measures that may affect human rights must be necessary and proportionate. This translates, among other things, into two important rules:

- the more invasive an investigate measure, the more serious the investigated crime must be, and

- the more invasive a measure, the stronger the safeguards must be.

For example, access to subscriber data could be made possible for a broader range of offences than access to or interception of traffic or content data. The latter should be limited to serious offences – and not be made a mandatory measure but one that States may choose to take, provided strong safeguards are in place.

Moreover, all investigative measures should be expressly limited in scope and duration – the treaty should thus require parties to establish scope and temporal limits for ongoing measures concerning any form of access to, production or acquisition of any types of private communications and personal data in criminal investigations, and to put in place measures to ensure those limits are adequately respected and enforced.

In terms of safeguards, decisions about invasive investigative measures should not be left to the law enforcement officers running an investigation. There needs to be a layer of independent oversight and authorization. In line with the second rule above, oversight and prior authorization requirements need to be stronger the more rights-intruding the measures taken are. Access to and interception of traffic and content data must have strong requirements of independent prior authorization (ideally of a judicial body) that should be clearly set out in the treaty itself.

With regard to international cooperation, the treaty must ensure that it does not create an avenue for circumventing domestic rights protections. First of all, no State should be expected to provide assistance to another for investigating actions that are lawful within its own jurisdiction. A dual criminality requirement should be firmly anchored in the treaty. Second, accessing data in another State should not be easier than domestically: at a minimum, all conditions and procedures applicable to domestic cases within the requesting state should apply here as well.

Moreover, the executing State should have a responsibility to evaluate requests for compatibility with human rights standards, and to refuse requests on such grounds where applicable.

All conditions and safeguards that would apply domestically in the executing State should also apply in cases of mutual legal assistance. This is particularly important given that the level of human rights protections and procedural safeguards can vary significantly between States.

Should the treaty allow State authorities to address data requests directly to companies and other third parties within another State's jurisdiction, the latter's authorities and oversight bodies should be empowered to assess the legality and validity of the request. Private parties have generally not sufficient capacity and lack the legitimacy to carry out such tasks with potentially far-reaching human rights impacts.

In concluding, allow me to invite you to seek out our Office's afore-mentioned submission to the Ad Hoc Committee, our previous oral statements, and our reports on the right to privacy (A/HRC/51/17, A/HRC/48/31, A/HRC/39/29; A/HRC/27/37) for more details on human rights considerations relevant for drafting a new cybercrime treaty. We look forward to the coming two days and stand ready to assist all interested stakeholders in elaborating human rights respecting and promoting responses to cybercrime.