1st intersessionals consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Panel "Criminalisation"

23 March 2022

Delivered by Paulina Gutiérrez

ARTICLE 19 welcomes the opportunity to participate in the first instersessional consultation of the Ad Hoc Committee. ARTICLE is a global human rights organisation that works around the world to protect and promote the right to freedom of expression and information ('freedom of expression'). Established in 1987, ARTICLE 19 monitors threats to freedom of expression in different regions of the world, and develops long-term strategies to address them. We advocate for the implementation of the highest standards of freedom of expression, nationally and globally. ARTICLE 19 has closely followed the process relating to this international instrument and has, over the years, had the opportunity to analyse several proposed and existing cybercrime laws around the world for their compliance with international freedom of expression standards. We are grateful for the opportunity to share our experience and provide some evidence based insight on how to ensure a human rights compliant treaty.

My presentation will focus on two key issues:

1. Some key observations on the proposed instrument based on our experience of analysing cybercrime laws;

2. The problems with including speech offences among "cybercrime" offences and some consideration upon offences that could and should not be included.

ARTICLE 19 is not persuaded there is a need for a convention on cybercrime. We are concerned that such a convention could be subject to abuse, and would perpetuate many of the current problems in existing national 'cybercrime' laws around the world. During the last ten years, we have raised concerns

about existing cybercrime laws that are open to abuse due to their vague terminology and lack of sufficient redress mechanisms. Therefore, ARTICLE 19 warns about the attempts to replicate several of those concerns and reminds the principle whereby the rights that people have offline must also be protected online.

As a matter of principle, any proposed convention should put human rights at its center and States should ensure all of its provisions are human rights compliant. This means that existing human rights principles and obligations governing international human rights law are taken as an applicable framework whereby States determine the scope of and necessary limitations under the treaty.

We have worked worldwide to analyse numerous proposed and existing cybercrime measures, including legislation in Bangladesh, Brazil, Cambodia, Ethiopia, Iran, Kenya, Mexico, Pakistan, Sudan or Thailand. These types of laws have also comprised an important component of submissions in the Universal Periodic Review of UN Member States such as Sudan, Cambodia, and Tanzania. ARTICLE 19 in 2015 submitted comments to the UN Special Rapporteur on freedom of expression for his comprehensive report on anonymity and encryption.Throughout our extensive monitoring of these cybercrime laws, we have noted three main problematic trends for freedom of expression:

1) The application of these cybercrime laws has been **used to criminalise ordinary activities**, including legitimate expressive activities involving computers. This is a growing, problematic trend in many countries around the world. Broad and vaguely-defined provisions that do not require “serious” harm or “dishonest”/”malicious” intent may be used to criminalise legitimate expressive activities involving computers, content-based conduct, or activities such as security testing, research, and the sharing of passwords for academic or personal use. Further, these cybercrime type laws often disregard the public interest defence that is necessary to prevent the abuse of cybercrime laws against individuals or organisations who expose violations of rights, corruption, dissenting views against public institutions or figures, discrimination, abuse, or fraud.

2) Second, the terms used in these laws are **routinely vague and subject to abuse.** This allows for an overbroad application of the laws, making them a dangerous tool for governments to use to crack down on freedom of expression and to criminalise opinions. These include terms such as “hate speech”, “cyberbullying”, “unauthorised” or “without authority” (typically not clearly defined in law, and are ambiguous as to who is required to provide relevant authorisation or authority); ‘critical information systems’ or ‘protected systems’ (referring systems that are essential to society or defence, but in reality, are often applied loosely and subject to abuse in order to protect public authorities from criticism).

3) Third, **content based offences often fail to comply with the three part test for restrictions on the right to freedom of expression**. Cybercrime laws containing overbroad speech offences, such as those related to terrorism and extremism, disinformation, ‘hate speech’, incitement or morality are frequently misused to imprison those critical of authorities or dissenting voices, or even block entire platforms. Provisions on different types of ‘hate speech’ do not sufficiently distinguish between the severity of the expression and its impact, and therefore fail to adequately determine proportionate sanctions that comply with international human rights standards. The trend concerning the use of vague and broad terms in cybercrime laws and “cyber” related criminal provisions is often accompanied with a clear focus on making the use of a computer, device or technology an aggravating circumstance. This is problematic from the point of proportionality of sanctions. There is no evidence that justifies the need to criminalise the use of technology -and therefore the means of expression- based on broad and vague expressive terms. The failure to properly define content

based offences puts a wide range of expression, including for example controversial political and artistic expressions, at risk of criminalisation. In other cases, these laws have extended protection to a wide range of State institutions and public officials from online offence and insults.

Based on ARTICLE 19's experience analysing and monitoring the implementation of cybercrime laws and "cyber" related offences around the world, we consider that **criminal sanctions in cyberspace must be strictly limited in number, scale, and scope.** Therefore the offences that could and must not be included in such a convention are the following:

- Core cybercrimes contained in Articles 2 to 6 of the Budapest Convention can serve as a reference point as a limit in scope and in requiring that any offences, at a minimum, serve legitimate aims and be necessary and proportionate. Duplicative offences raise the risk of prosecution for the same conduct as multiple different crimes, as well as increase the risk of overinterpretation and abuse.

- "Cybercrime" must not be used to prosecute content-based offences. From a human rights perspective, the scope of the UN Convention should be narrow and should not include speech-related offences. Just because a crime might involve technology does not mean it needs to be included in the proposed convention. Under international law, restrictions on freedom of expression must satisfy a three-part test. If expressive activities are criminalised as part of a cybercrime proposal, those measures constitute restrictions under international law and must satisfy the tripartite test. Measures that broadly restrict any form of content in a cybercrime law are unlikely to advance a legitimate aim, nor be necessary or proportionate. For the avoidance of doubt, restrictions on the use of encryption or anonymity tools constitute restrictions on freedom of expression and must be avoided at all costs. This is consistent with international human rights standards in this area. Finally, all prohibitions of 'hate speech' and incitement to violence should not fall under the scope of a criminal cybercrime treaty. International human rights law provides extensive interpretative guidance for States to follow, in particular under Article 19 and 20 of the ICCPR. Instead of discussing the inclusion of 'hate speech' and incitement related crimes under this convention, States should comply and implement recommendations outlined in the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, in the reports of the UN Special Rapporteur on freedom of expression and other standards in this area.

The recommendations outlined earlier are part of ARTICLE 19's 10 recommendations and you can find details on our statement on our website.