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

## Introduction

***Derechos Digitales*** is a non-profit non-governmental organization founded in 2005, with ECOSOC consultative status. We are dedicated to the defense and promotion of human rights in the digital environment, especially those related to freedom of expression, privacy and access to knowledge and information.

*Derechos Digitales* welcomes the opportunity to contribute in this Second Session, according to the operative paragraph 8 of the General Assembly Resolution 75/282[1] and the Ad Hoc Committee Chair's Notes on the modalities of multi-stakeholder participation[2]. In this contribution, we would like to emphasise some points according to the items discussed about the topics of "Criminalization" and "Procedural measures and law enforcement", as follows.

## 1. Provisions on Criminalization:

### Safeguarding human rights in the digital age:

1. In a joint civil society letter by *Derechos Digitales* and more than 130 NGOs and experts in more than 56 countries, we caution against casting too wide a net when deciding what crimes to include within this new treaty[3]. Just because digital technology is used in the commission of a crime does not make that act a cybercrime, nor should the simple use of technology in the commission of an offense be an aggravating factor. The future treaty should protect and safeguard human rights both against the threat of cybercrime and against the possibility of state abuse in the investigation and prosecution of those crimes.

2. Cybercrime laws must not be enacted, used and abused to criminalise legitimate activities, such as pursuing public interest. In the past few years, different actors and Human

[1] A/RES/75/282. Available at: https://undocs.org/en/A/RES/75/282
[2] Modalities of the participation of multi-stakeholders in the Ad Hoc Committee. Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Modalities_multi-stakeholders_Chairs_note.pdf
[3] Derechos Digitales. Solicitamos a la ONU garantías de derechos humanos en tratado de"ciberdelincuencia". Available at: https://www.derechosdigitales.org/17961/organizaciones-de-sociedad-civil-solicitamos-a-la-onu-garantias-de-derechos-humanos-en-tratado-sobre-ciberdelincuencia/

Rights mechanisms expressed in different situations how cybercrime national legislation and practices can undermine human rights, target human rights defenders, civil society organisations, digital security researchers, whistleblowers and journalists, and allow abuses.[4] To prevent criminal legislation from being professionally or voluntarily dedicated to improving the security of computer systems, if it is necessary that the crime of illicit access has as a requirement a volitional component that points to the bad faith of the action.

3. For instance, as the Special Rapporteur on the rights to freedom of peaceful assembly and of association reported: "*A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world*"[5]. We see several cases show the high risks to human rights in the use of state surveillance technologies on a mass scale[6].

4. We understand that in an eventual convention Members States should ensure that any normative proposal is consistent with the obligations of States before international human rights law and to oppose any proposal contrary to it. Preventing cybercrime can not be an excuse to allow State mass surveillance tools that undermine human rights[7]. Principles of legality, necessity and proportionality should be the minimum standards.

## Protection of encryption to foster human rights:

5. Encryption and anonymity enable individuals to exercise their human rights in the digital age. According to the Special Rapporteur of Privacy, "*encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection*"[8]. As David Keye noted: "*Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law*"[9].

6. Criminalyzing privacy and anonymity protection technologies, such as virtual private networks or VPNs and the use of encryption tools, does affect everyone who uses these technologies to defend their privacy and fight cyberspace surveillance.

---

[4] For example, the cases and problems reported by the United Nations High Commissioner for Human Rights, regarding "The right to privacy in the digital age", A/HRC/48/31. Available at: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F48%2F31&Language=E&DeviceType=Desktop&LangRequested=False

[5] A/HRC/41/41. Available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/41

[6] The cases led to the reaction of the United Nations, for example, the General Assembly Resolutions about "The right to privacy at the digital age": A/RES/68/167, Available at: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F68%2F167&Language=E&DeviceType=Desktop&LangRequested=False. A/RES/73/179. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/449/97/PDF/N1844997.pdf?OpenElement

[7] General comment no. 37 on the right of peaceful assembly (article 21,ICCPR), CCPR/C/GC/37, para 60 and 61.

[8] A/HRC/29/32. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[9] Ibid.

**The crimes should be "core cybercrimes", with narrow, precise and specific well defined scope:**

7. We understand there are risks of a very broad approach and the scope of sanctioned conduct. Creating broad new crimes has no justification, since most of them are already determined in other statutes. Crimes that are the subject of other discussions, such as conduct in the content of communications, such as hate speech or the infringement of intellectual property, should not, but could be used to silence and persecute activists, journalists and marginalised communities.

8. Determining the crimes in an eventual convention should be focused on the pursuit of acts whose object of protection or whose object of attack is properly related to information and communication technologies. An eventual cybercrime convention is not the place to create new broad crimes. Broad crimes should be avoided, since it can punish even unintentional figures, and without distinguishing the information class from the form to access it. This means that the act of knowing or using information, without hacking anything, becomes a cybercrime.

9. Precision and clear delimitation of cybercrimes is essential for an eventual convention. The focus should be on "core cybercrimes", with a "narrow set of offences inherent to cyberspace", as recommended by the Office of the High Commissioner for Human Rights last January[10].

10. There is a risk to human rights when it is proposed to include in this treaty the crimes related to content (speech-related crimes) imposing undue restrictions on freedom of expression[11]. As civil society worldwide can attest, the national laws on cybercrimes that include content-related crimes can be and are used to persecute those who criticize the authorities or the dissenting voices, or even to block internal platforms. In our opinion, "cyber-enabled" crimes should not be considered cybercrimes just because of the use of ICTs in their commission, given the risk of basing cooperation on a potential cybercrime treaty for prosecution of crimes that are not unique to ICTs across borders. The activity of utilizing the capabilities of ICTs themselves for the purpose of safeguarding human rights and protecting communications, as is the case with the use of anonymity and encryption technologies, must not be criminalized or considered as an aggravating circumstance. The same is true for deployments of technology with the purpose of investigation of vulnerabilities, collection and dissemination of publicly relevant information (as a content-related crime), and other activities by researchers, journalists, and human rights defenders.

[10] OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal Purposes. Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

[11] OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal Purposes. Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

## 2. Procedural measures and law enforcement:

### All investigations should guarantee due process and fair trial:

11. Pursuing cybercrimes requires the capacity to investigate and identify criminals. But state investigations and identifications can not be done at the expense of human rights and fundamental guarantees. Collecting personal information in cross borders investigations and using sophisticated surveillance technologies are a serious risk to privacy and due process. Communications surveillance through the use of hacking tools represents a highly invasive activity that also endangers security. Mass surveillance is contrary to human rights. States can not turn citizens into suspects, without a crime involved.

12. The eventual convention should have strong safeguards in the cooperation, procedural measures and law enforcement, since there are several risks to privacy and creation of new sources of vulnerability.

### Principles of legality, necessity and proportionality, and judicial authorization, oversight and accountability:

13. Several cases in Human rights courts and expert bodies express that it is an interference with human rights accessing personal data by public authorities'. So while this access may be justifiable, it will always have human rights implications including across borders. Any interference in the right to privacy needs to comply with the principles of legality, necessity, and proportionality. Procedural and investigative measures should have a precise and narrow scope.

14. A potential future convention should determine at least the minimum guarantees to prevent the abuse of those investigative techniques that are harmful to fundamental rights, such as: judicial authorization, ideally in advance, but at least in a later form; to establish that any order imposing the measures should be limited in time and precise about the measure duration; establish that once the deadline indicated for the reservation of the investigative measure has been fulfilled, the citizen can be notified; strengthen the notification requirement for someone affected by an interception measure, so that it is effectively complied with. Judicial authorization, oversight and accountability are needed to protect the right to privacy.

15. A key component of the proportionality of any investigative measure is the determination of the amount and type of data that is necessary to effectively investigate cybercrime. We must highlight, in accordance with several organizations and experts around the world, that government access to communications data, including metadata and subscriber data, can be as intrusive as access to communications content or even more so. A future convention must acknowledge that access to metadata is therefore by itself a measure that can gravely impact the right to privacy, and should therefore be subject to high levels of scrutiny and procedural safeguards.