DataPrivacyBR Research

Submission by Data Privacy Brasil Research Association to the United Nations Ad-Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

April 08th 2022

The Data Privacy Brasil Research Association welcomes the opportunity to submit its contribution towards the second session of the Ad-Hoc Committee on Cybercrime. We also reiterate the joint letter endorsed by 134 civil society organizations and experts in more than 56 countries and sent to the chairperson of the Ad-Hoc committee[1].

About Data Privacy Brasil Research Association

Data Privacy Brasil Research Association is a Brazilian non-profit civil society organization founded in 2020 that promotes the protection of personal data and other fundamental rights in the face of the emergence of new technologies, social inequalities and power asymmetries. We have a multidisciplinary team from different Brazilian regions that develops public interest research and advocacy.

About this document

There is no consensus on how to tackle cybercrime at the global level or a common understanding or definition of what constitutes cybercrime. From

[1] Letter to the United Nations to Include Human Rights Safeguards in Proposed Cybercrime Convention: https://direitosnarede.org.br/2022/01/13/letter-to-the-un-ad-hoc-committee-on-cybercrime/

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

DataPrivacyBR Research

a human rights perspective, it is essential to keep the scope narrow. Thus, Data Privacy Brasil Research Association wishes to address the items related to **criminalisation** and **law enforcement** in these recommendations.

Our understanding is that **cybercrime is based on three criteria: malicious intent, large scale effects and violation of fundamental rights**. In this sense, we advocate in favor of principles related to the protection of personal data, that is, **a flow of data consistent with human rights** and harmonized with practices and norms already consolidated by States and the private sector at a global level.

We strongly oppose expansive interpretations of cybercrimes and methods of cooperation by authorities that may violate fundamental rights, especially in a Latin American context with authoritarian pasts and police procedures that often evade legality.

I. Criminalisation

The definition of cybercrime is usually related to crimes committed via the Internet or computer systems. However, the direct relationship of this type of conduct must be considered, at a global level, together with the protection of human rights, while at the same time creating a balance with security issues. Therefore, **a strict definition of "cybercrime" is necessary, based on three elements: i) malicious intent; ii) exploitation of computer systems with large-scale effects; and iii) violation of fundamental rights.**

Thus, the first observation is that the intention of the agent is a crucial part of the definition since in online practices there can be similar conducts that will have completely opposite consequences. Researchers that investigate breaches in order to warn people about risk or cybersecurity agents, for example, cannot be mistaken by malicious agents that will search for breaches and use them to benefit themselves and harm others.

A second point to be highlighted is that the use of Information and Communications Technologies (ICTs) cannot be a sole criteria for

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

DataPrivacyBR Research

criminalization[2]. Also, crimes that already exist in international and local legal instruments (*cyber-enabled*) should not be considered cybercrimes just because ICTs were implemented in the execution - which is also a point of great divergence between the States and would hinder the practical approach of the present legal instrument. Considering the international scope of the convention and possibility of collaboration between countries, the effects of the use of computer systems must have a large scale effect and a significant impact on societies.

The last remark is that any activity of conduct utilizing ICTs for the purpose of safeguarding human rights must not be considered a cybercrime. This limit to the definition is essential to avoid the wrongful criminalization of human rights defenders such as journalists, activists, academics, whistleblowers, etc[3]. Any type of online actions taken in order to protect human rights and principles, such as freedom of opinion and expression, freedom of information, right to association, right to privacy, non discrimination and dignity of the human person, should not criminalize the agent, especially under cybercrime provisions just because it envolved the use of ICTs[4] and practices of data scraping, search for vulnerabilities in computer systems, disclosure of information that is of public interest, amongst others.

The wrongful criminalization of human rights defenders and state abuse[5] has been seen before due to cybercrime legislations in different countries[6]. That said, **by narrowing the scope of the convention it would be possible to reduce the risk of negatively**

[2] There is consensus on activities made possible by the use of ICTs that are not considered cybercrimes, such as SPAM, as already shown in a 2013 UNODC study: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

[3] Abuse of Cybercrime Measures Taints UN Talks. HRW, May 5, 2021. Available at: https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

[4] Negotiations Over UN Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights. EFF, March 3, 2022. Available at: https://www.eff.org/deeplinks/2022/03/negotiations-over-international-police-powers-agreement-must-keep-human-rights

[5] Computer crime: the necessary human rights perspective. Digital Rights Lac, November 22, 2013. Available at: https://digitalrightslac.derechosdigitales.org/en/delitos-informaticos-la-necesaria-perspectiva-desde-los-derechos-humanos/

[6] The report *How journalists and human rights defenders are targeted online* from Access Now shows how vague legislations, such as some of the cybercrime laws, can be used to target human rights defenders. See the report here: https://www.accessnow.org/cms/assets/uploads/2019/06/MENA-report.pdf

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

impacting citizens and agents involved in human rights preservation. We reinforce the need to guarantee that these agents are not punished, especially cybersecurity researchers and whistleblowers[7] that sometimes can make similar actions as the individuals with malicious intentions commiting actual cybercrimes.

We understand that it is not up to the Convention to address illicit conduct related to disinformation within the concept of cybercrime, not even in additional protocols.

The Convention should not include infringement of copyright and related rights by means of ICT within the scope of criminalization (*Chapter II*) or illegal use of software for copyrighted computer systems or databases, considering that intellectual property legislation already addresses such issues.

II. Law Enforcement

Some types of cybercrimes related to content are already quite consensual and have consolidated legislation, such as online child sexual abuse material. In that sense, the discussion of safeguards and limits for State action is essential to promote an update of current practices without leaving aside the guarantee of the right to privacy and data protection and, at the same time, avoiding greater abuses by the State in their execution[8]. Nevertheless, the Convention cannot prevent States from bringing additional safeguards, based on their domestic legislations[9].

Requests related to cybercrimes must target specific accounts and individuals. There must be reasonable justification based on

[7] The necessity to protect whistleblowers was already in discussion in the Recommendation CM/Rec(2014)7 of the Committee of Ministers of the Council of Europe. The document can be accessed here: https://rm.coe.int/16807096c7

[8] In this way, the Convention follows a continuity of protection of Human Rights, already established by the Budapest Convention. Available in: https://rm.coe.int/1680081561. Accessed on April 5th, 2022.

[9] This is of paramount importance for countries such as Brazil and EU Member States, for example, which are pioneers in global advances in digital rights and protection of fundamental rights online. See: The Brazilian Civil Rights Framework for the Internet ("Marco Civil da Internet" - Law 12965/2014), here http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm; and the Declaration of Digital Principles and Rights by the European Commission (2022) here https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

concrete facts, particularity and seriousness; there must be a mechanism for review; and oversight by an independent authority. That is because the disproportionate and unspecific coverage of the use of information and communication technologies can impact the right to privacy and freedom of expression of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, and many others.

The Convention must provide robust procedures for cybercrimes investigations, including cooperation between different states and authorities. Principles already listed in international treaties on the flow of personal data must be respected, harmonizing the future text with existing practices. Investigations must have prior judicial authorization, so that data are obtained and processed fairly and lawfully. There must be express provision regarding specified and legitimate purposes for the collection, access and processing of personal data, ensuring their adequate, relevant and not excessive use in relation to the purposes for which they are stored.

Massive data scraping, surveillance and other abuses in investigations, including access to metadata, must be avoided. These data collection processes pose risks for activists, journalists, social movements, researchers and journalists, and cannot be used to limit human rights under the pretext of combating cybercrime.

We agree with the Electronic Frontier Foundation and Privacy International that the proposed convention should explicitly recognize that access to communications data, including metadata and subscriber data, can be as intrusive as access to content. The massive collection of metadata **impacts the fundamental right to the protection of personal data**. As a matter of due process and the rule of law, methods of cooperation that involve extracting and sharing metadata must have a demonstration of public reason related to an ongoing investigation, necessity, legality, and proportionality.

International cooperation needs to be effective under a narrow scope of cybercrimes and well-defined procedures, in order to avoid abuses in requests. In this sense, the principled basis of data protection is effective for guaranteeing human rights in

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

instruments already consolidated such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights instruments and standards. The provision of **principles such as data quality, purpose, necessity and proportionality guarantee greater transparency** in the cross-border flow of personal data and efficiency in the cooperation established between investigative authorities.

The Convention, therefore, can harmonize guarantees and rights of personal data, facilitating cooperation between authorities to deal with crimes classified according to the three aforementioned characteristics. Based on existing instruments such as Convention 108, which was aimed at relations between State and citizens, the idea here is to transpose this reasoning to relations between States, when it affects citizens.

The Convention cannot prevent countries from creating additional safeguards to prevent setting exceptional parameters for massive metadata collection and limiting "fishing expedition" without due process. States should have the right to create procedural mechanisms centered on fundamental rights to allow the collection of data in real time, within clearly defined situations of transnational crimes that require these methods of investigation.

The Convention should not impose obligations of legislative measures necessary to empower competent authorities to collect or record traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system **without clear principles of necessity, legality and proportionality**.

We understand that when the requested telematic data are associated with personal data that may contribute to the identification of the user or the terminal, the requesting authority must also justify the need for the measure for the specific investigation, which must be subsidiary in relation to other means of proof that are less burdensome to the rights of third parties and the relevance of the information obtained in relation to the investigated fact, which must be specified as much as possible

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

based on identifying and contextual elements relating to the possible illicit act.

Chapter III cannot take a focus on technical means obligations without a concern for fundamental rights and due process as a starting point.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org