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

June 30th 2022

The Data Privacy Brasil Research Association welcomes the opportunity to submit its contribution towards the third 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

Data Privacy Brasil Research Association wishes to address the item related to **"Preventive Measures"**, following our first submission[2] and

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

Contato
contato@dataprivacybr.org

dataprivacybr.org

[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/

[2] 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 8th, 2022: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Data_Privacy_Brasil_Research_Association.pdf.

DataPrivacyBR Research

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

Contato
contato@dataprivacybr.org

dataprivacybr.org

understanding that cybercrime is based on three criteria: malicious intent, large scale effects and violation of fundamental rights.

First, we will focus on the issue of data retention, bringing important conceptualizations and due process measures essential for the protection of fundamental rights. Then, we reinforce the need for the inclusion of human rights principles and protection of personal data, as already internalized by other international instruments, and how the education and training of authorities is a preventive and essential part of the effectiveness of this Convention.

I. Data retention

In the context of definitions and debates about data collection and content data, a distinction and important clarification about data collection for investigations is necessary.

Data retention should be a legal obligation directed to application service providers limited to register system traffic data for a defined period of time, that is to say that the content of the message/activity is not retained. It distinguishes itself from the acquisition of data which should be a result of a judicial order to a third party to authorize the register of specific data regarding a determined individual or group, and also limited in time.

This distinction is necessary because, in the acquisition context, the content could be accessed, and **if there is no separation between the concepts, there could lead to access to content information without a judicial authorization**. Since the collection of information regarding communication and activity online can bring a risk of excessive surveillance, the access to the contents of these communications can be even more harmful when not controlled. That said, if both concepts are looked at as the same, doors will open for unsanctioned collection and storage of data, raising the risk of fundamental rights violations.

In that sense, it is necessary to note that the **bulk collection of data must be prohibited. It is an unproportionate risk for the population to support and goes against the presumption of innocence**. Additionally, as mentioned before, fundamental rights and principles such as dignity of the human person, liberty, personal data protection, right to privacy and others will be harmed.

DataPrivacyBR Research

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

Contato
contato@dataprivacybr.org

dataprivacybr.org

Considering that the present contribution regards criminal investigations and criminal procedures related to cybercrimes, it is also essential to mention the **due process and the legal reserve as guiding principles on the matter**. The collection and any other processing of data needs to be regulated in order to preserve both principles. The access to content, which is very delicate information, needs to be regulated by the judicial body that will authorize this type of surveillance only when it is crucial data for the case. Under this supervision, there will be criteria for the collection, there will be a specific target and a specific time frame in which the actions to obtain the information will take place. And before that, there will be a procedure stated by law that will condition the collection to the judicial authorization.

In a broader perspective, an independent oversight, that will be explained below, can be a useful tool to guarantee that the State is following through with the obligations defined by the Convention and that the public authorities are meeting their purpose.

II. Capacity building for law enforcement authorities

Awareness and education are key to preventive measures for all actors in the digital ecosystem. In the case of the Convention, educating and training authorities becomes essential for the treaty to be truly effective. **Preventive measures must be applied both to the State**, in terms of incident response teams and information security measures, **and to citizens** who must have their fundamental rights protected, especially on cross-border access to electronic evidence.

We reinforce the importance of maintaining personal data protection principles and, consequently, fundamental rights, in criminal investigation processes between jurisdictions. Besides, the Convention should be in line with international human rights standards, including the 1948 Universal Declaration of Human Rights, the 1966 United Nations International Covenant on Civil and Political Rights, the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the 1989 Convention on the Rights of the Child, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the 2019 UN Resolution "The right to privacy in the digital age" (A/HRC/RES/42/15), and other international human rights instruments.

DataPrivacyBR Research

These instruments shall incorporate the **principles of proportionality, legality, and necessity**, in the protection of privacy and personal data. In this way, some instruments of preventive measures must include encryption and anonymity, in the data collection phases, and **must not oblige treatment agents to decrypt data**, as already stated by the joint submission of Electronic Frontier Foundation and Privacy International[3]. The Brazilian Supreme Court recognized that encryption is an essential component of the fundamental right to privacy and that digital rights must be understood as fundamental rights[4].

Encryption and anonymity are part of a democratic society, ensuring essential rights for public life. They allow the development and sharing of opinions, as well as contribute to the safety of journalists, activists, and minorities who suffer some type of repression. Although these instruments are also used for illegal weapon sales, drug sales and child abuse streaming, this is a duality already recognized by the UNODC Global Program on Cybercrime[5], which should be considered through other investigative tools. Once identification becomes necessary for the cross-border access to electronic evidence, measures of **purpose and proportionality must be prioritized** throughout the process of international cooperation.

We reinforce that training of authorities and due process will only be fully effective if there is a **common understanding of cybercrimes** and the concepts used in process definitions. Also, the Convention cannot prevent States from bringing additional safeguards, based on their domestic legislation, and give them the right of refusal to cooperate, in particular when the protection of human rights might be at stake.

In order for there to be trust between all parties, an important preventive measure against violations of rights and abuses by the State is to have **independent oversight**. This could be made possible either by the UN itself, such as through the UNODC Global Program on Cybercrime or through independent data protection authorities. Having independent oversight

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

Contato
contato@dataprivacybr.org

dataprivacybr.org

[3] Submission by Electronic Frontier Foundation and Privacy International to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/EFF_contribution.pdf.

[4] Opinion of the Brazilian Supreme Court (ADPF 403): https://lapin.org.br/wp-content/uploads/2020/08/Voto-Min-Fachin-ADPF-403.pdf

[5] Global Programme on Cybercrime: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

will bring **transparency and legitimacy** to the Convention and its signatories, for cross-border processes as well as public-private cooperation.

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

Contato
contato@dataprivacybr.org

dataprivacybr.org