Asociación por los Derechos Civiles **April 30th, 2021**

6th Round of Consultations on the 2nd Additional Protocol to the Budapest Convention on Cybercrime

Asociación por los Derechos Civiles (ADC) is a civil society organization founded in 1995 to defend and promote fundamental rights in Argentina and Latin America, with special focus on the needs of those in vulnerable situations due to their gender, nationality, religion, disability condition, among others.

We welcome this new opportunity to provide comments and before going on to the observations, we would like to thank the work done by the Commission, as well as for opening these spaces for public participation. In the same vein, we would especially like to highlight the inclusion of a chapter on safeguards and conditions relating to the protection of personal data.

Now we want to use this new round to further previous remarks that have not yet been solved and address recent topics added to the protocol.

a. **Section 2: Procedures enhancing international cooperation between authorities for the disclosure of stored computer data**

Art. 6: Request for domain name registration information and art. 7: Disclosure of subscriber information

As explained in the explanatory report in paragraph 93, this section seeks to find a rapid and effective mechanism for cooperation where the authorities of one Party can request domain name registration and subscriber information to private entities located in the territory of another party. Nevertheless this information could be obtained through MLA or procedure established in article 18 of the Convention, it was considered important to set up this complementary mechanism that would

enable more effective cross-border access to information needed for specific criminal investigations or proceedings.

Although we agree on the need to have agile and efficient procedures that allow for an effective criminal investigation, we have certain reservations as to which authority should be empowered to carry out the procedures.

Competent Authority

Both Article 6 and Article 7 procedures provide that the request may be issued by the competent authority designated by the Party. In turn, Article 3.2.b defines ‘’competent authority’’ as "a judicial, administrative or other law enforcement authority that has the authority under domestic law to order, authorize or carry out the execution of the measures provided for in this Protocol for the purpose of gathering or presenting evidence in connection with specific criminal investigations or proceedings."

As this section applies whether or not there is a mutual assistance treaty or arrangement between the Party seeking the information and the Party in whose territory the private entity is located, the intervention of an independent judicial or other authority of a similar nature is essential to control the legality in the process and protect rights of individuals. As we stated in previous comments, the adoption of a broad criterion of authority for the issuance of measures with limited safeguards is extremely risky for the rights of individuals. Under this rule, local or municipal authorities, police or anybody freely determined by the state party will have the legitimacy to communicate directly with the service provider and compel it to provide sensitive information. Thus, there may be situations in which access to or transfer of data occurs without the intervention of any independent public body capable of assessing the legality of the order.

In this respect, article 7.2.b establishes the possibility for each Party to declare that the order under article 7.1 must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent

supervision. We suggest, to guarantee a minimum legal control, that this provision should be mandatory for all procedures under Section II.

Subscriber information

We understand the definition of subscriber information used in the convention[1] allows this concept to include possibly sensitive information, which is why the requirement of a judicial or independent authority becomes especially relevant.

In this manner, we insist that clarity in the definition of the term "subscriber information" is key to distinguish information that is less intrusive to privacy from information that poses serious risk to it. In that sense, we maintain our concerns stated in previous comments about the risk that data revealing behaviours, habits or other characteristics of a person's private life may be included under this category. Particularly, IP addresses shouldn't be included under the category "subscriber information". For instance, when they are delivered by providers other than those providing the telecommunication service, IP addresses constitute traffic data insofar as they are part of the information produced within - and referring to - the communication made by the person with a user or with a given service. But even when this information is provided by the ISP, it can reveal intimate details about a person's location, customs, or everyday actions[2]. Therefore, the important issue is not if some information can be considered or not "subscriber information" but if such information could pose a serious risk to the right to privacy. In this regard, the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights considered that targeted surveillance is "generally protected in criminal proceedings or other kinds of investigations, and involves collecting and/or monitoring the communications of an identified or identifiable individual, and IP address, a specific device, a specific account, etc."[3]. Therefore, such measures constitutes an "interference with individual's privacy"[4] and their legitimacy must be

[1] art. 18.3 of the convention and paragraph 92 of the explanatory report
[2] What an IP Address Can Reveal About You. A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, May 2013 https://www.priv.gc.ca/media/1767/ip_201305_e.pdf
[3] Standards for a free, open, and inclusive Internet. Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression, paragraph 210 http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf
[4] Ibid, paragraph 215

considered on the basis of the tripartite test, which states that the measure must be legal, necessary for a democratic and proportionate society. Under this principle, IP addresses should always be required by judicial order.

Although art. 9.b recognizes this possible problem and allows the Parties to make a reservation in this regard, we understand that it should not be a power of the Parties, but an express limitation to protect the rights of individuals.

b. <u>Section 3: Procedures enhancing international cooperation between authorities for the disclosure of stored computer data</u>

Art. 9 Expedited disclosure of stored computer data in an emergency

The channel established in this article is intended to be a faster and simpler mechanism to cooperate in an emergency. Among the features that make it faster is that it is not necessary for a request for mutual assistance to be prepared in advance.

According to the Explanatory Report in paragraph 153, it's up to the Parties to decide the use of this new channel or the Emergency Mutual Request, based on their accumulated experience and the specific legal and factual circumstances at hand. However, this decision incorrectly assumes that the choice is only a matter of convenience. Actually, the Emergency MLA process demands certain formal steps - such as prior mutual assistance requests - that encourages compliance with minimal safeguards. On the contrary, the real-time exchange of information may allow state parties to easily avoid compliance with data protection rules or other fundamental rights. Therefore, the protocol must assume that this new channel is more challenging -in terms of protection of rights- than the Emergency MLA channel. Thus, the choice should not depend on the discretion of the states but on the fact that the emergency situation possesses some conditions that makes it different from the emergency that authorizes the use of Emergency MLA. Such qualities may be provided by requiring that the imminence or risk be imperative or compelling. Another way would be to demand that the requesting state has to prove that it's impossible or useless to use the Emergency MLA channel due to the sensitivity of the case. For the same reason, only a judicial or similar independent authority should have the faculty to issue the request.

c. **Section 5 Procedures pertaining to international cooperation in the absence of applicable international agreements**

Art. 12 Joint investigation teams and joint investigations

Art. 12 states that the decision to create or join a JIT will be made by the "competent authority" determined by each State Party. While this provision may be grounded in the diversity of legal systems, we consider it's not a reason to prevent the protocol from requesting that such authority be a judicial one or another authority with the same degree of independence. Agreements to implement JITs are very sensitive because it defines the conditions and procedures of the operations and thus, it may affect people's fundamental rights. Therefore, there must be strong oversight over the necessity and legitimacy of the operation which should be carried by a judge or by an impartial authority.

Additionally, the protocol should require that the purposes of the agreements be drafted in the clearest, most detailed and specific manner. And if there is any doubt about the interpretation of a term, the answer should be to restrict the use of evidence to other uses or different cases.

d. **Chapter III Conditions and safeguard**

Even though articles 13 and 14 establish conditions and safeguards that include protection of personal data, we suggest more requirements may be demanded in order to protect individuals rights.

In addition to this, there are safeguards that can be added to the Convention, such as the following:

-Request all the state parties to the passing of data protection law in accordance with high international standards. Convention 108 and 108+ would be useful for this subject.

-Allowing the access to data prior review by a judicial court or other independent and impartial authority.

-Requesting the notification to the person whose data has been granted access, insofar as it doesn't jeopardize the investigation. If that is the case, the individual

should be informed immediately after the danger has ceased. In this sense, article 14.11 establishes the necessity of transparency and notice. However, the disclaimer about ‘’reasonable restrictions under its domestic legal framework’’ should be clarified in order to avoid abusive restrictions.

In last, recent adoption of the General Comment 25 (2021) on children's rights in relation to the digital environment compels us to pay attention to the protection of the data of children subject to criminal investigation. For this reason we suggest that the protocol considers this new situation by introducing specific safeguards. In this respect, paragraph 47 of the General Comment 25 may be relevant as it establishes: ‘’Digital technologies bring additional complexity to the investigation and prosecution of crimes against children, which may cross national borders. States parties should address the ways in which uses of digital technologies may facilitate or impede the investigation and prosecution of crimes against children and take all available preventative, enforcement and remedial measures, including in cooperation with international partners. They should provide specialized training for law enforcement officials, prosecutors and judges regarding child rights violations specifically associated with the digital environment, including through international cooperation’’.

For more information, contact Valeria Milanes, Executive Director, vmilanes@adc.org.ar , Alejo Kiguel, Ssr. Project Officer, akiguel@adc.org.ar , or Eduardo Ferreyra, Ssr. Project Officer, eferreyra@adc.org.ar