November, 2019

Dear Nina Lichtner.

I am sending this e-mail on behalf of Asociación por los Derechos Civiles (Association for Civil Rights), NGO based in Buenos Aires, Argentina, in relation to the call for written comments by stakeholders and consultations at the Octopus Conference in the process for Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime.

About ADC

The 'Asociación por los Derechos Civiles' (Association for Civil Rights) or ADC (Spanish acronym), is a civil society organization that has been working since 1995 defending and promoting the exercise of civil and fundamental rights in Argentina and Latin America, with special focus in the needs of those in vulnerable situations due their gender, nationality, religion, disability condition, or deprivation of liberty.

Over these years, ADC raised strategic allegations of human rights violations, promoted legal and institutional reforms aimed at improving the quality of Argentinian democratic institutions and influenced positively in public policymaking processes. This activity has been recognized at a national and international level for its expertise and efficacy in the defense and promotion of civil rights and democratic values. ADC also has stood out in its fight for the promotion and defense of the founding principles of the Rule of Law.

In line with this trajectory, ADC has remained at the forefront of the human and civil rights defense in different political, social and cultural contexts, in both Argentina and Latin America. Thus, aware of the increasing digitalization and the use of technology in the various public and private fields, ADC has undertaken the mission of understanding the impact of digital technologies on human rights.

Background on the matter

During 2017-2018 we developed a research about Cybercrime and Human Rights in Latin America, with special focus on digital evidence and the use of technologies in the criminal procedure. As a result, we realised a series of reports:

- Digital Evidence, Investigation of Cybercrime and Criminal Process' Guarantees (here)

-The Budapest Convention on Cybercrime and Latin America. Brief guide on its

impact on people's rights and guarantees. Volume 1 (here)
-Computer Forensic Research in Latin America. Volume 2 (here)
-Legal analysis of the situation of digital evidence in the criminal process in Argentina. Volume 3 (here)

Because of our work on the subject, we were granted a thematic hearing before the IACHR (here)

More reports on topics related to the use of technologies in criminal investigations can be found in our web site.

At the same time, we developed profuse work on data protection. See for example:
-Your digital self: Discovering the narratives about identity and biometrics in Latin America (here)
-Initial analysis of Argentina's personal data protection bill (here)
-Comparative analysis between the GDPR and the national law on the protection of personal data (here)
-ADC Comments on the Personal Data Protection Bill (here)

We are currently research (early stages) on topics related to the request and use of personal data in criminal procedures and its implications to rights and guarantees.

Our interest and request for your consideration
We are quite interested in participate in the discussions de CoE is promoting on the matter, in the process of the preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime.

In that sense, if we are accepted, we would truly appreciate to receive information in advance about the Octopus Conferences and/or workshops and/or work meetings and/or written or virtual processes in which we can follow up and provide feedback to the discussion as a civil society voice.

Having this information in advance would allow us to make a proper follow up to the different discussions as well as take budgetary provisions for attendance at meetings, if necessary.

Preliminary remarks on the draft texts on "Direct disclosure of subscriber information" and on "Giving effect to orders from another Party for expedited production of data"

Without prejudice to the research we are carrying out -which will allow us to make

greater contributions later- based on the work we have done so far, we share the following preliminary comments.

-Subscriber information concept: The provision of subscriber information is subject to a more permissive legal regime as regards the guarantees to be respected. The reason for this decision is that access to this kind of information would be less intrusive. However, the definition of the term "subscriber information" in the Budapest Convention is not specific enough to clarify certain doubts. Particularly, we are concerned about the risk that data revealing behaviours, habits or other characteristics of a person's private life may be included under this category. Therefore, the protocol should be clearer about the definition of "subscriber information" and thus seize the opportunity to clarify doubts not resolved by the provisions of the Budapest Convention.

In this sense, a first step would be to make it expressly clear that -at least- IP addresses do not fall within the category of "subscriber information". When they are delivered by providers other than those providing the telecommunication service, IP addresses constitute traffic data insofar as they form part of the information produced within - and referring to - the communication made by the person with a user or with a given service. But beyond that, what makes this kind of information sensitive is that it can reveal intimate details about a person's location, customs, or everyday actions. Thus, there is an intense intrusiveness to the privacy of individuals.

This reasoning has been supported by the Inter-American Human Rights System. The Inter-American Court of Human Rights has held that the right to privacy applies not only to the content of a communication but also to "technical operations designed to record this content". The court also held that "the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content (...) or other aspects inherent in the communication process,such as those mentioned". (Escher et al. v. Brazil , 114)

Moreover, 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." (highlighted is our 2016 Freedom of Expression and Internet Report, paragraph 210). Therefore, such measures are considered to be an "interference with individual's privacy" (ibid, para. 215) and their legitimacy must be considered on the basis of the tripartite test, which states that the measure must be legal, necessary for a democratic and proportionate society. Similar conclusions can be drawn from the European and universal systems.

As we said before, the regime provided for in the current article 4 of the protocol establishes a regime with limited guarantees under the argument that data relating to subscribers does not significantly affect the privacy of individuals. However, the absence of a precise characterization of the data that fall into this category means that IP addresses - which may reveal sensitive information about people's privacy - can be accessed without the required safeguards. That is why it would be desirable to establish a clear definition of "subscriber information" that restricts the scope to specific assumptions and excludes sensitive data such as IP addresses or others that allow conclusions to be drawn about the privacy of individuals.

Competent authority: For its part, it would be desirable for the protocol to establish in a mandatory manner the need for an independent judicial or other authority of a similar nature to intervene in the process of issuing the order by the requesting state, either by issuing the order or by authorizing the issuance by another authority.
Art. 4 leaves it to each state party to take the necessary measures to grant its "competent authorities" the power to issue orders to service providers located in another territory to provide subscriber information. At the time of establishing what is meant by "competent authority", the Convention does not provide any kind of definition. However, the Explanatory report (paragraph 138) argues that the term refers to a judicial, administrative or law enforcement authority that is empowered by national law to issue such measures.

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 any body freely determined by the state party will have the legitimacy to communicate directly with the service provider and compel it to provide subscriber 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.

While the article does not preclude states parties from requiring the order to be issued by a prosecutor or other judicial authority, or under independent supervision, such a provision is not mandatory but depends on the decision of each state party. It is therefore recommended that a mandatory rule for all states be the intervention of an independent or similar judicial authority that guarantees minimum legality control for

the issuance of orders that are themselves subject to a soft regime of guarantees.

Looking forward for your answer.

Valeria Milanes
Executive Director
Asociación por los Derechos Civiles
vmilanes@adc.org.ar

Eduardo Ferreyra
Project Officer Ssr.
Asociación por los Derechos Civiles
eferreyra@adc.org.ar