December 14th, 2020

Contribution by Asociación por los Derechos Civiles to the 5th Round of consultations on the 2nd Additional Protocol to the Budapest Convention on Cybercrime

Asociación por los Derechos Civiles (ADC) welcomes this new opportunity to provide comments on the draft provisions of the Second Additional Protocol to the Budapest Convention on Cybercrime. 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. During the 4th round of consultations, we submitted our written comments and now we want to use this new round to further our previous remarks and address the recent topics added to the protocol.

3 Joint investigation teams and joint investigations

The draft 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 -as stated by 3.1.2- and thus, it may affect people's fundamental rights. Therefore, they cannot be left exclusively to low-level officials or those with a particular interest in the investigation, such as prosecutors. There must be strong oversight over the necessity and legitimacy of the operation. This oversight can only be carried out by a judge or by an impartial authority.

Also, we believe that section 3.1.2 should have a mechanism for safeguards and protection of rights. As currently drafted, it seems that the procedure and conditions of JIT's operations are left to the discretion of the agreement determined by the competent authorities. The absence of limits in terms of fundamental rights or data protection may transform the use of these agreements as a tool to bypass compliance with essential procedures and guarantees. This problem is aggravated when the section does not determine who the "competent authorities" will be, since there is the possibility that such important agreements are entered into by authorities that do not have the required independence and impartiality.

The article also allows States participating in a JIT to benefit from the production of investigative measures without the need to make a request for mutual assistance. This is another reason to require that the authorities responsible for entering into such an agreement be judicial or similar authorities. Otherwise, this mechanism may become an incentive to circumvent the usual procedures.

When determining the use of the evidence produced by the participating authorities, the section allows other Parties to use it for the purposes for which the agreement has been entered into, provided that the agreement does not set forth terms for refusing or restricting use. This attempt to limit the use of evidence may be futile if the purposes of the agreement are drafted in ambiguous or vague terms. Therefore, 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.

We believe that "safety of a natural person" (paragraph 5) should be understood as serious bodily harm. Although this clarification is included in the Draft Explanatory Report, we think the protocol should include it in its main text to clear up any doubt about its interpretation. Finally, the duty of the participating authorities that received the information or evidence to notify the participating authorities that provided the information or evidence without undue delay should be mandatory, not optional.

4 Direct disclosure of subscriber information

As stated in our written comments for the 4th round of consultations, 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 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. 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[1]. 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."[2]. Therefore, such measures constitutes an "interference with individual's privacy"[3] 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.

Under this principle, IP addresses should always be required by judicial order and state parties shouldn't have the option to choose otherwise. Also, the authorities of the state where the requested service provider is located should also be notified simultaneously of the order. This provision is included in the protocol but only as an option to the state parties when signing or ratifying the Convention. To provide

[1] *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

[2] *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

[3] Ibid, paragraph 215)

adequate safeguards to individuals, this notification should be mandatory, so States can check the necessity or the proportionality of the order.

Another topic addressed in our previous comment is the definition of “competent authority”. We would like to reiterate that the Convention should require that judicial authority or another national independent body be the only ones empowered to issue such measures. Otherwise, local or municipal authorities, law enforcement agencies or any body designated by the state will be able 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 authorities with enough expertise and impartiality to review the legality of the order.

6.Request for domain name registration information

Paragraph 4 states that the information disclosed in response to a request shall be subject to appropriate safeguards. We welcome this provision, particularly, because it enshrines the need to take into account data protection law. We think this can be a great opportunity to incorporate data protection provisions not only for this case but for all the data processing established by the Budapest Convention. The draft announces that a text on the subject is currently being drafted. We suggest to consider the Convention 108 and 108+ as a basis for that text. And also, it would be convenient to request all the state parties the passing of data protection law -if they currently don't have one- and/or the ratification of the Convention 108 and 108+.
In addition to this, there are several safeguards that can be added to the Convention, such as the following:
-Limiting the access only to data of persons suspected of taking part in the investigated crime.
-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.

-Incorporating basic principles of data protection law such as the need for the collection of personal data to be adequate, relevant and necessary for the purpose of the processing.
-Setting up a data protection officer or some authority with expertise in data protection in the requesting party as well as the requested party. They must take part in the procedure conducted by competent authorities in order to oversight the proportionality of the orders, requests and transfer of data.

7. Expedited disclosure of stored computer data in an emergency

According to the Explanatory Report, it's up to the Parties to decide the use of this new channel or the Emergency Mutual Request. But 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.

8 Emergency mutual assistance

As we stated before, the definition of emergency (paragraph 1) should be clarified in order to avoid ambiguities. Particularly, the concept of "safety" must be interpreted as avoiding serious bodily harm to a natural person. While this is included in the explanatory report, we suggest to incorporate it to the main text.

Paragraph 3 grants the possibility to State Parties to require appropriate levels of security and authentication before accepting an EMA request. We recommend this requirement be mandatory, so all requests be provided with proper technical security measures.

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