kaspersky

Comments Submitted to the Cybercrime Convention Committee (T-CY) of the Council of Europe

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Draft Protocol version 2)

Kaspersky's Submission

May 2021

Kaspersky is grateful to the Cybercrime Convention Committee (T-CY) for the opportunity to provide comments to the Draft text of the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (further – 'Draft text').

We support the important work the T-CY undertakes for developing an international framework for cross-border cooperation, including between public and private parties, for combatting cybercrime. Recognizing the growth of more sophisticated and targeted cyber threats[1], we at Kaspersky provide our comments below to certain parts of the draft text, and would be happy to take part in further consultations with stakeholders to develop a balanced proportionate response to cyber threats and to ensure effective criminal justice measures on cybercrime, taking into account the protection of human rights and fundamental freedoms.

1. Service providers need to be provided with rights to challenge and/or object to orders requesting disclosure and/or provision of data

Establishing clear lawful procedures to raise concerns and to challenge requests is important for service providers should they see the fulfilment of orders as actions that could possibly undermine the integrity of their services, or if fulfillment comes up against conflicting domestic legal regimes and, therefore, conflicting regulatory compliance. Therefore, for effective fulfillment of orders, and effective access by the requesting authorities to evidence, service providers need to be provided with clear means and lawful procedures to challenge as well as to object to orders requesting the disclosure and provision of information if the following of such orders does not seem possible, as explained by the service providers.

These procedures should indicate reasonable timeframes for service providers to take steps if they want to challenge the request(s). Within these timeframes, service providers would be able to consult with independent authorities and/or legal parties before implementing the orders to ensure the trust in, and integrity of their services.

---

[1] Kaspersky Security Bulletin 2020. Statistics https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/

kaspersky

2. Service providers need to have lawful means to be transparent about the orders received and therefore to notify their users

The right to be transparent about the requests and their implementation by service providers is crucial for ensuring user trust in, and integrity of providers' services. What is more, in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[2] (Article 8 on 'Transparency of processing' and Article 9 on 'Right of the data subject'), service providers need to be able to satisfy user requests and/or notify them of any orders seeking access to their data, unless these orders are accompanied by a relevant court order prohibiting such notice. The explicit addition of these rights for service providers would not only help ensure trust in their services, but would also help enhance the trust in law enforcement powers through ensuring that the following of the orders is legitimate, lawful and proportionate, as it avoids infringing fundamental rights.

3. Joint investigative measures need to be limited to those that are authorized under domestic laws of all participating Parties

Taking into account the different legal regimes among participating Parties, certain measures being strictly prohibited in certain participating Parties may be permitted in others and therefore there could be a risk that the investigative measures, as provided in Article 12, may potentially go further than it is authorized under the domestic laws applicable to the territory where the investigation is carried out. Furthermore, given the global nature of modern information and communications technology (ICTs), the joint investigative measures may also affect data and/or communications of users located in Parties that do not participate in joint investigations and thus violate those users' fundamental rights.

Therefore, it is important to limit the investigative measures outlined in Article 12 to those that are authorized under the domestic laws of all participating Parties to prevent the violation of laws applicable to the territory where the investigation is carried out, as well as the violation of international human rights law.

4. Participation of private-sector actors in joint investigations needs to be clarified

Joint investigative measures of participating Parties may include engagement with the private sector, including relevant service providers, since the private sector owns and/or manages modern ICT-related services. However, the role and expected participation of the private sector actors is not provided or clarified in the Draft text, which puts the private sector into a legal 'grey zone'. For ensuring the transparency and legitimacy of public-private cooperation in obtaining lawful evidence to combat cybercrime, it is crucial to explicitly clarify the expected role and actions from the private sector actors as well as their participation in cybercrime investigations.

[2] https://rm.coe.int/16808ade9d

kaspersky

5. Mandatory prior review by a judge or other independent oversight authority is needed for authorizing disclosure of data to ensure the necessary data protection safeguards

We note that the Draft Protocol lacks necessary data protection safeguards while providing provisions for authorizing the disclosure of information, including personal data. For instance, Article 9 – on expedited disclosure of stored computer data in an emergency – may potentially authorize the disclosure of content data and/or personal data, while, at the same time, Article 9 does not provide clarity on legal consequences if the data disclosed is misused further (or, particularly, is not deleted after serving the initial purpose) by the requested Party. In this regard, we support the view of the European Data Protection Board[3] that the "systemic involvement of judicial authorities in requested Parties is essential to ensure an effective compliance review of the requests with the Convention and to preserve the application of the principle of double criminality in the field of judicial cooperation". What is more, in order to respect the individuals' fundamental rights as well as ensure the security of data processing (and avoid data breaches), mandatory judicial review and cooperation with judicial authorities would serve in this regard as a necessary data protection safeguard.

Therefore, a mandatory prior review by a judge or other independent oversight authority in authorizing the orders for the disclosure of data would serve as an essential data protection safeguard, and thus would also help enhance trust in law enforcement activities in combatting cybercrime through obtaining electronic evidence.

To discuss the contents of the comments or request additional information, please contact Anastasiya Kazakova, Senior Public Affairs Manager at Kaspersky (anastasiya.kazakova@kaspersky.com).

[3] https://rm.coe.int/edpb-statement022021onbudapestconventionnewprovisions/1680a1617f