INFORMAL MEETING OF THE JUSTICE AND HOME AFFAIRS MINISTERS

Bucharest, 7-8 February 2019

Working lunch

"Gathering electronic evidence in criminal matters: protecting the rights of individuals in cyberspace through an effective criminal law response in line with rule of law and fundamental rights requirements"

Cybercrime and the question of gathering electronic evidence raise challenges for criminal justice of unprecedented magnitude and complexity. The vast majority of criminal investigations involves evidence on computer systems, but the evidence needed may be located on servers in foreign, multiple or unknown jurisdictions. Very often the evidence needed is held by multi-national service providers which may be offering their services for profit in a particular Member State while being based in another jurisdiction and their data being stored in a third jurisdiction.

More than half of all criminal investigations require cross-border access to electronic evidence and very often through cooperation with multi-national service providers (see the Commission's Impact Assessment[1] accompanying the e-evidence package).

Security and fundamental rights are not in opposition but interconnected. Governments have the obligation to uphold the rule of law and to protect individuals and their fundamental rights and freedoms against crime also in cyberspace, including through an effective criminal justice response, such as production orders for electronic evidence and cooperation with service providers. This was stated already in 2008 by the ECtHR in the case K.U. v. Finland[2] when the Court considered that "*practical and effective protection of individuals require effective steps* - including adequate legislation in place - *in order to identify and prosecute the perpetrators*. […] *It is the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context*".
If volatile electronic evidence cannot be secured effectively, if only a small share of cases of cybercrime is prosecuted and adjudicated and if large numbers of investigations of criminal offences are abandoned for lack of access to evidence, governments may fail in their obligation to protect individuals and their rights.

New solutions are needed to cope with the new realities of cyberspace. Law enforcement and judicial authorities must be able to gather electronic evidence from all relevant sources and, in particular, to have effective access to information held by service providers, also in a cross-border context. Such collection and access must meet fundamental rights and rule of law, including data protection, requirements, and take into consideration that service providers may be exposed to conflicting legal obligations.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN
[2] http://hudoc.echr.coe.int/fre?i=001-89964

The "Council conclusions on improving criminal justice in cyberspace", adopted by the JHA Council on 9 June 2016[3], during the Netherlands Presidency of the Council of the EU, stressed "*the importance of protecting cyberspace from abuse and criminal activities for the benefit of our economies and societies, and therefore the need for law enforcement and judicial authorities to have effective tools to investigate and prosecute criminal acts related to cyberspace*". The Council concluded, inter alia, that "*cooperation with service providers is to be enhanced*", among other things, through quicker disclosure of data by service providers.

The Council noted "*that cyber-enabled and cybercrime violate fundamental rights and freedoms, and the need to ensure full protection of these rights and freedoms*" and recognised "*that the use of investigative measures should be guided by the protection of fundamental rights and freedoms and the principles of necessity and proportionality*".

Since the JHA Council of June 2016, several proposals have been developed or are in preparation to address these questions. They include in particular the proposals for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, the accompanying Directive on legal representatives and the discussion about the possible adoption of decisions for the opening of negotiations on an agreement of the European Union with the United States of America and on a Second Additional Protocol to the Budapest Convention on Cybercrime.

Moreover, a number of decisions related to electronic evidence have been issued by the Court of Justice of the European Union such as Case C-207/16 Ministerio Fiscal[4] and the European Court of Human Rights decision on Benedik v. Slovenia[5] (see the discussion paper of the Cybercrime Convention Committee with a brief review of relevant court decisions[6]). These decisions demonstrate the complexity of the matter of access to electronic evidence – further compounded by questions of jurisdiction and cross-border access to "data in the cloud" – and the need to reconcile security and the protection of fundamental rights when developing new procedural rules.

The Presidency strongly believes that the proposed Regulation on gathering electronic evidence in criminal matters, on which the Council reached a general approach in December 2018 under the Austrian Presidency, will enable more effective criminal justice in cyberspace by providing effective tools for obtaining evidence while ensuring the protection of fundamental rights and while meeting the rule of law requirements of necessity and proportionality. That version, which includes a balanced notification mechanism and other safeguards, represents a solid basis for negotiations with the European Parliament that should start as soon as possible[7].

To build on and complement the e-evidence Regulation, the negotiation of a Second Additional Protocol to the Council of Europe Convention on Cybercrime, as well as future international agreements with third countries, in particular with the USA, should ensure a comprehensive international legal framework on the matter in line with rule of law requirements and contributing to the protection of fundamental rights.

---

[3] https://www.consilium.europa.eu/en/press/press-releases/2016/06/09/criminal-activities-cyberspace/#

[4] http://curia.europa.eu/juris/document/document_print.jsf?docid=206332&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=658573

[5] http://hudoc.echr.coe.int/eng?i=001-182455

[6] https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472

[7] In its Conclusion from 18 October 2018 (EUCO 13/18) the Council underlined the need for a swift adoption of the e-evidence proposals by the end of this legislature; https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf

The Commission will have the opportunity to inform the Ministers about the proposals to the Council for negotiating directives on the international aspects of this file.

An enhanced dialogue is required with parliaments, private sector and civil society in view of greater awareness and a better understanding of the rationale of the solutions proposed, that is, protecting individuals against crime effectively and protecting their rights at the same time.

Against this background, the Presidency would like to invite Ministers to share their views regarding:

- the specific ways for continuing the dialogue and raising awareness on the proposed E-evidence package and the safeguards foreseen;

- a first exchange of views on the issues to be considered in future international agreements in this area.