Commission Proposes Legislative Framework for E-Evidence

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2018, Vol. 13(1) eucrim pp 35 – 36
ISSN: 1862-6947
https://eucrim.eu

On 17 April 2018, the European Commission tabled legislative proposals that frame EU law allowing European law enforcement authorities to quickly and more efficiently secure and obtain electronic evidence ("e-evidence"). There was much debate in the run-up to the proposal, with calls for legislative action being uttered by the Council, on the one hand, and doubts by private companies and civil society organizations being voiced about the need for such action, on the other (see also eucrim 4-2017, p. 178).

The measures now proposed by the Commission consist of a "Regulation on European Production and Preservation Orders for electronic evidence in criminal matters" (COM(2018) 225) and a "Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" (COM(2018) 226).

The core measure is the proposal for a Regulation. It lays down EU-wide binding rules under which law enforcement authorities in the EU can order a service provider offering services in the Union to produce or preserve electronic evidence in cross-border situations. The main feature is that requests can be directly submitted to the private companies, irrespective of the location or storage of the data and without involving foreign state authorities in the first place.

Although the Regulation is inspired by the principle of mutual recognition, it shifts away from the traditional approach of European cooperation in criminal matters. The place of the storage of the data is no longer the decisive factor for jurisdiction, but instead the sole criterion is the private entity's operation in the EU.

The Commission argues that the use of traditional measures of mutual legal assistance (MLA) are slow and cumbersome if law enforcement authorities intend to obtain data stored in electronic form, such as IP addresses, e-mails, documents in clouds, etc. Furthermore, public-private cooperation has proven inefficient, since it often relies on a voluntary basis, in particular if the service provider is based in a third country, e.g., the United States.

Another main problem is the lack of legal certainty, since national obligations for service providers to cooperate with law enforcement authorities are fragmented.

As a result, the proposal aims at the following:

- Adapting cooperation mechanisms to the digital age;
- Improving legal certainty for authorities, service providers, and persons affected;
- Maintaining sufficient safeguards for the rights and freedoms of all concerned.

The main *contents* of the proposed Regulation are the following:

- Establishing a European Production Order allowing a judicial authority in one EU Member State to request e-evidence (e.g., e-mails, texts, or messages in apps) directly from a service provider irrespective of the location of the data;
- Obliging the service provider, in principle, to transmit the requested data to the issuing authority within 10 days at the latest, within 6 hours in case of emergency;
- Establishing a European Preservation Order allowing a judicial authority in one EU Member State to oblige a service provider to preserve specific data in order to enable the authority to request this information subsequently via MLA, a European Investigation Order, or a European Production Order;
- Carrying out the preservation without undue delay and, as a rule, upholding it for 60 days.

The proposal for a Regulation sets out several *conditions and safeguards*. These are as follows:

- The orders can only be used in criminal proceedings, thus excluding their use for preventive purposes;
- The orders need to be validated *ex ante* by a judicial authority;
- The orders only apply to stored data, thus excluding real-time interception of telecommunications;
- The measure is limited to what is necessary and proportionate for the purposes of the relevant criminal proceedings;
- A European Production Order requesting transactional or content data can only be issued for "more serious offences," i.e., offences punishable in the issuing state by a custodial sentence of a maximum of at least three years or for specific cybercrime-related or terrorism-related offences as referred to in the proposal (while an order for subscriber and access data and a Preservation Order can be issued for any criminal offense);
- Limited possibilities of the service provider to object to a European Production Order, e.g., if the order is formally incomplete or unspecific, in case of *force majeur*, *de facto* impossibility, a manifest violation of the Charter of Fundamental Rights of the EU, or a manifest abuse;
- Establishment of specific review procedures in favour of the service providers if the obligation to provide data conflicts with competing obligations from the law of a third country, e.g., the USA;
- Persons affected by the measure, e.g., customers of the service provider, are ensured to have the protection laid down by the EU's data protection law (Regulation 2016/679 and Directive 2016/680) plus the right to an effective remedy against the European Protection Order. Another provision proposes that immunities and privileges, which protect the data sought in the Member State of the service provider, be taken into account by the court in the issuing Member State if it assesses the relevance and admissibility of evidence.

If the service provider does not comply with an order by the deadline or without providing sufficient reasons, an enforcement procedure is triggered involving the competent authorities of the EU Member State where the order has to be enforced. The enforcing authority may also deny the request on the basis of very limited grounds for refusal.

The proposal for the Directive on legal representatives aims at overcoming current different approaches of EU Member States towards imposing obligations on service providers in criminal proceedings, depending on whether they provide services nationally, cross-border within the EU, or from outside the Union. Therefore, the Directive makes it mandatory for service providers to designate a legal representative in the EU to receive, comply with, and enforce orders on gathering e-evidence.

The proposal already faced criticism from civil society organizations and business associations. They argue that it cannot be up to private companies to decide on the right balance between law enforcement and the fundamental rights of citizens. Furthermore, the new proposal would undermine existing MLA procedures

and give up most of the achieved MLA principles. They also pointed to the European Investigation Order as an already existing, efficient MLA instrument that could be improved in the future but does not need to be replaced by the European Production Order. Others consider the proposal to be opening "Pandora's box," since it is an incentive for other countries, less committed to the rule of law (such as Russia, Turkey, or China), to act in the same way and therefore jeopardize European companies. Business organizations expect economic losses for the service providers, since they may no longer protect their customers' interests appropriately. Ultimately, some critics argue that the effects of the e-evidence measure may be low, since criminals will seek and find other ways to escape access to their data by law enforcement authorities.

Notwithstanding this criticism, the EU is in a tight spot, since the USA adopted the so-called CLOUD Act enacted in March 2018. "CLOUD Act" stands for "Clarifying Lawful Overseas Use of Data Act". Its purpose is similar to the e-evidence proposal of the European Commission. It allows U.S. federal law enforcement to compel U.S.-based technology companies, via warrant or subpoena, to provide requested data stored on servers – regardless of whether the data are stored in the USA or on foreign soil. It also foresees that, by means of "executive agreements," law enforcement authorities from foreign "qualified countries" will have equal access to the data of the U.S. companies.

Furthermore, the Council of Europe is currently preparing an additional protocol to its 2001 Cybercrime Convention, which addresses e-evidence. Accordingly, law enforcement authorities may directly cooperate with providers of other jurisdictions. International production orders shall modify the existing MLA and make the fight against crime speedier and effective.

The legislative proposal on e-evidence comes with a series of measures presented on 17 April 2018. The package of measures was entitled "Denying terrorists and criminals the means and space to act".

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union