Further Concerns of EP Against E-Evidence Legislative Proposal

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

The EP rapporteur in the LIBE committee responsible for the Commission proposal on law enforcement access to e-evidence, *Birgit Sippel* (S&D, Germany), voiced further criticism (see already eucrim 4/2018, 206). After a first working document (see ibid), *Sippel* and co-rapporteurs/shadow rapporteurs examined the following issuesin several subsequent working documents:

- The scope of the application and the relation of the proposed instrument to other European instruments;
- The role of service providers;
- Relationship with third-country law, in particular the U.S. CLOUD Act;
- Conditions for issuing European Production Orders and European Preservation Orders and Certificates (EPOC(-PR)s);
- Safeguards and remedies;
- Enforcement of EPOC(-PR)s

AUTHOR

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

ISSN: 1862-6947
https://eucrim.eu

Scope of application and the relation of the proposed instrument to other European instruments

In part A of the so-called "2ndworking document" of 6 February 2019, *Sippel*and co-rapporteur *Nuno Melo* (EPP, Portugal) doubt whether the envisaged regulation on European Production and Preservation Orders for electronic evidence in criminal matters can be based on Art. 82 TFEU since it is not an instrument of mutual recognition which involves direct cooperation between judicial authorities, but concerns the execution of law enforcement orders by private providers. Furthermore, the EP rapporteurs stressed that it "needs to be made unequivocally clear" whether a Regulation is the right instrument or whether not a Directive is appropriate for an e-evidence legal framework.

Part B of the 2ndworking document concludes that as regards subscriber data – "the data category required the most in trans-border cases, and needing swift action in order to start a criminal investigation and identify a suspect or link a suspect with a certain communication" – both the European Investigation Order and the CoE Cybercrime Convention represent a "forthcoming framework" despite their limitations.

Role of service providers

In the third working document of 13 February 2019 (part A), Sippel and co-rapporteur *Daniel Dalton*(ECR, UK) question, *inter alia*, whether a fully-fledged fundamental rights assessment can and should be outsourced to private service providers. In this context, they note:

"The question of the possibility of outsourcing, even privatising, state prerogatives and sovereignty, relates to core (constitutional) prerogatives of a state, such as the protection of the fundamental rights of its citizens

by its national constitutional provisions/traditions and international instruments, as well as the protection against potentially unjustified encroachments of foreign authorities on its territory in the judicial/law enforcement field."

Therefore, the question is whether the judicial authority of the state of enforcement need to be stronger involved.

In addition (part B of the third working document), the EP rapporteurs request the establishment of a reimbursement regime for the service providers. Finally, service providers need full legal certainty when it comes to their obligations and liability; they should not be left in a legal limbo between law enforcement/judicial orders, data protection obligations and third country laws. *Sippel*and *Dalton*conclude that "the proposed Regulation, however, seems to unfortunately exacerbate the legal uncertainty for the service providers."

Relationship with third-country law, in particular the U.S. CLOUD Act

In the fourth working document of 11 March 2019 (Part A), Sippel and co-author *Sophie in't Veld* (ALDE, Netherlands) analyse the effectiveness of obtaining relevant e-evidence data by means of existing instruments of judicial cooperation, in particular by the 2003 EU-US Mutual Legal Assistance Agreement. They conclude that the MLA scheme is working satisfactorily. Therefore, a new instrument on direct access to e-evidence seems questionable where subscriber, access, and transactional data are concerned (at least when the major US providers are involved). As regards content data, improvements in the MLA agreement could be realised. In addition, the EU-US MLA agreement leaves enough room for strengthening judicial cooperation. According to the working document (Part A) the problem is not the legislative side, but the adequate outfitting of judicial authorities handling MLA requests with adequate financial, human, and technical resources.

Part B of the 4th working document provides an in-depth look into the contents of the U.S. CLOUD Act (see also *Daskal*, eucrim 4/2018, 220-225). Sippel and in't Veld conclude that an EU e-evidence instrument would imply several incompatibilities with the US act and ultimately lead to conflicts of law. They also oppose Commission plans to get a mandate for negotiations with the USA – on behalf of the EU – on an executive agreement within the framework of the CLOUD Act. In view of the pending e-evidence proposal, this seems, *inter alia*, premature, as a number of questions have not yet been sufficiently answered before entering into negotiations with the USA.

Many shortcomings were also found in relation to Arts. 15 and 16 of the proposed e-evidence Regulation (Part C of the 4th working document); these provisions introduce a review procedure for cases in which the service provider, requested to produce data based on an EPOC, is faced with conflicting obligations from third-country law (e.g., if the service provider has its main seat in the third country).

Conditions for issuing EPOC(-PR)s

In Part A of the 5th working document (8 March 2019), Sippel and co-rapporteur *Cornelia Ernst* (GUE/NGL, Germany) critically remark that the proposed rules on the issuing authority, which also entitle prosecutors to issue EPOCs/EPOC-PRs in cases of subscriber and access data, do not fully take into account constitutional constraints in many EU Member States. The authors fear a race to the bottom, which is why the necessity of judicial authorisations must also be considered in view of access data.

In view of the offences justifying the issuance of EPOC(-PR)s, there are concerns (as already mentioned in previous working documents) over reducing the protective role of authorities in the executing state. The proposal is a fundamental shift away from the existing *acquis*in judicial cooperation. The rapporteurs advocate the introduction of a stronger notification system with the right of the executing state to check, e.g., whether immunities or privileges are affected or whether the measure would be admissible in a similar

domestic case (as provided by the EIO). They also advocate the right to oppose an EPOC(-PR) (see also Part B of the 5th working document). The latter should at least be possible when fundamental rights obligations are at stake. A double criminality test should take place if an EPOC refers to transactional and content data.

As further outlined in Part C of the 5th working document,*Sippel* and *Ernst* also voice concern over the total exclusion of the executing authority from being involved in proportionality checks. This also represents a paradigm shift from mutual recognition. It deprives the enforcement of coercive measures of the necessary checks and balances. Since the proportionality test seems the only safeguard against misuse, it might be advisable to think about more detailed and common rules on proportionality.

Safeguards and remedies

Inconsistencies with existing mutual recognition instruments, e.g., the EIO, and the fact that the executing authority is kept out, also cause problems when it comes to notification of the data subject. In Part A of the 6th working document of 1 April 2019, Sippel and *Romeo Franz* (Greens/EFL, Germany) stress that EU legislation should introduce several parameters to resolve the tension between the interests of law enforcement authorities in withholding notifications and the data subject's interest in exercising his/her rights to defence and fair trial. It should be borne in mind that – according to the Commission proposal – it is only up to the issuing authority to inform.

In Part B of the 6th working document, Sippel and Franz examine the necessary *ex ante* safeguards, i.e., safeguards that must be guaranteed before e-evidence is collected and transferred to the issuing authority. The MEPs also found that *ex ante* safeguards necessitate stronger involvement of authorities in the executing state, including a comprehensive notification system and the possibility of a meaningful reaction to EPOC(-PR)s. Relevant rules could be modelled on Art. 31 and Art. 11 of the EIO Directive. A fundamental rights clause should be worded along the existing clause in the EIO Directive.

Such a notification mechanism triggers the question of which state must be notified. In order to guarantee efficient legal remedies, the "affected state" must be defined.

The effectiveness of remedies also plays a vital role for *ex post* safeguards. As further outlined in Part C of the 6th working document, Sippel and Franz question whether the data subject should have the right to not only challenge the legality of an EPOC in the issuing Member State, but also in the Member State of residence and/or the Member State of enforcement. Furthermore, the e-evidence proposal triggers the question of whether harmonised rules on legal remedies should be brought forward. The MEPs further note that the question of harmonisation is also raised for admissibility/exclusionary rules in the e-evidence context. The new EU tool must, however, at least specify which remedy applies if e-evidence has been obtained illegally.

In addition, *Sippel* and *Franz* identify further gaps in the Commission proposal, such as the prohibition of further processing and onward transfer of evidence, the inclusion of financial compensation and penalties for unlawfully acting issuing authorities, and remedies for service providers.

Ultimately, the MEPs fiercely reject the Commission's view (as mentioned in the impact assessment for the e-evidence proposal) that a "right to security" has to be balanced against other individual rights and safeguards. *Sippel*and *Franz*emphasise that such a position risks being below the level of the ECHR, where such a right has not been legally recognised. It cannot be part of a balancing test.

In the 7th working document of 1 April 2019, Sippel and *Ignazio Corrao* (EFDD Group, Italy) deal with several aspects of the enforcement of EPOC(-PR)s in the Commission e-evidence proposal. They first disagree with the Commission's approach on leaving sanctions against providers for non-compliance with their obligations up to the national laws of the Member States. They advocate "some sort of harmonisation of the sanctioning regime." One reason is the risk of "forum shopping," since service providers may appoint their legal representative in the Member State with the lowest sanctioning regime.

Another critical issue is the proposed deadlines within which service providers must enforce EPOCs (in principle, 10 days upon receipt; in "emergency cases," 6 hours). The first challenge is that the deadlines might be too short for service providers to assess the legitimacy of an EPOC. Second, small- and medium-sized companies (SMEs) may not be able to meet the deadlines since they do not run 24/7 services. The same is true for third-country service providers that operate in different time zones. Third, the deadlines are not realistic for guaranteeing fundamental rights protection (if it is shifted to private companies). Therefore, the proposed deadline system must be reconsidered, either by introducing two separate deadlines (one for big companies, another for SMEs) or by setting up longer deadlines.

The 7th working document ultimately notes that the objection mechanism for service providers triggers many legal questions. Many concerns were voiced in previous working documents, e.g., regarding the involvement of the executing State authorities, the scope of the refusal grounds, and the level of information necessary for the service provider to make a meaningful legality check.

In this context, Sippel and Corrao conclude: "All these options are closely connected with the more general debate about mutual recognition in EU criminal law. The viewpoints on this issue vary substantially across Member States, national authorities, the Commission, CJEU, EC[t]HR, scholars and practitioners, and it becomes clear that the principle of mutual recognition is still under construction, closely connected to the changing nature of EU integration."

In sum, the working documents of the MEPs address several critical issues already voiced by European bodies and non-governmental organisations (see details at eucrim 4/2018, 206; 3/2018, 162-163, and 2/2018, 107-108). After these considerations, the EP blocked further negotiations with the Council before the Parliamentary Elections in May 2019. The hot debate over whether the e-evidence proposal is necessary and, if yes, which content it should have will be resumed with the newly composed EP in autumn.

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