European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

8.3.2019

5th WORKING DOCUMENT (A)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Conditions for issuing an EPOC(-PR)s
Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit SippelCo-Author: Cornelia Ernst

Introduction

The present working document provides an analysis of the conditions for issuing European Production Orders and European Preservation Orders and Certificates (EPOC(-PR)s) in the issuing State. Consequently, it covers Articles 4, 5 and 6 of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)). Furthermore, some remarks concern the choice on the categories of data (Article 2 on definitions) inasmuch as they have an impact on the conditions for issuing an EPOC(-PR).

Remarks on specific issues

a) Status of the issuing authority (Art. 4)

According to the Commission proposal, an EPOC concerning transactional and content data may be issued by a court authority (namely a judge, a court, or an investigative judge). An EPOC-PR as well as an EPOC concerning subscriber data and access data may be issued, not only by those authorities, but also by a prosecutor. Furthermore, an EPOC on all types of data, as well as an EPOC-PR, may also be issued by any other competent authority acting in the capacity of an investigating authority in criminal proceedings, as defined by the issuing state. In this case, however, the EPOC and the EPOC-PR must be validated, after examination of its conformity with the conditions for issuing an order, by the competent authorities (i.e., only by court authorities for an EPOC on transactional and by content data and prosecutors in the other cases).

According to the explanatory memorandum of the Commission,[1] prior intervention of a judicial authority (judge or, for an EPOC on subscriber/access data and an EPOC-PR, a prosecutor) would be a satisfactory safeguard against infringements of fundamental rights. This is true in the case of those Member States where some types of data can already be requested by the police, without confirmation of a judicial authority. However, it ignores the obligatory court authorisation in other Member States for certain categories of data. Furthermore, it does not solve the issue of different roles of the prosecutor in the different Member States.

A prosecutor is, by definition, a party to the procedure with the obligation to prosecute and although functionally independent from the executive power (at least in most Member States), they are not impartial. It is a party to the procedure with the obligation to prosecute, despite the formal provision in many Member States that it shall collect evidence proving guilt as well as exculpatory evidence.

For this reason, in several Member States the prosecutor cannot order the most intrusive measures affecting fundamental rights, including measures affecting the right to privacy.[2] In

[1] P. 10.

[2] For this reason, one may also put into question the Commission's written reply following the shadows' meeting of 9 October 2018 (p. 10) stating that the prosecutor can be considered 'as judicial authority' in the meaning of an impartial court authority. Also the ECtHR clarified the issue that a prosecutor cannot be considered a court authority in the framework of Article 5 ECHR (right to liberty and security) and the notion "or other officer authorised by law to exercise judicial power" (see, ECtHR, *Medvedyev and Others v. France*, a. n.

order to request 'access data', for example, a court order is necessary in several Member States.[3] Even though 'access data', a new category introduced by the Commission, is often the first information necessary to investigate the case (for example, a dynamic IP address), certain transactional (traffic) data often has to be analysed for such data, as also recognised by the ECtHR.[4] In line with this recognition, and according to CoE Cybercrime Committee reports, there seems to be a growing trend across Member States that a court authorisation is necessary for such data.

Consequently, when it comes to the category of access data, the approach of the Commission, in its current form (supported by a majority in the Council in its General Approach), would substantially lower the constitutional requirements in several Member States. This could cause a direct clash between the national constitutional standards and the primacy of EU law. The primacy of EU law is a crucial EU principle that has been created by EU Court of Justice case-law. Some national constitutional courts have already expressed reservations regarding the potential lowering of national constitutional rights, through EU law, on several occasions.[5]

Therefore, in order to solve the situation and to avoid creating a race to the bottom where standards are concerned, any request for access data should be based on a court authorisation or validation. This is all the more true when one looks at the existing European Investigation Order (Directive 2014/41/EU) (EIO), which took a much more prudent approach. Upon insistence of the EP, in order to issue an EIO, the executing state may decide that an additional court authorisation in the executing state is necessary - in addition to the validation procedure in the issuing state by a judge or prosecutor (see Article 2 EIO). Applying this provision also for an EPOC(-PR) would add additional safeguards as regards to the respect of fundamental rights in the Member States. In view of the general trend across Member States regarding court authorisations for requests for access data, one might even argue that EU harmonisation for the category of access data has to be introduced through a general obligation of requesting a court authorisation for such data.

Moreover, also the validation test regarding the notion of "any other competent authority acting in the capacity of investigating authority in criminal proceedings" has to be further clarified, in order to make sure that a substantial validation procedure of the competent authority is carried out and that fundamental rights are fully guaranteed.

3394/03 and *Moulin v. France, a. n. 37104/06*).
Furthermore, one could also question the notion that the right to liberty is more important than the right to privacy as regards court authorization. Due to the advances and possibilities of new technologies (e.g. ranking systems applied in China based on behavioral monitoring through technology), more and more technologies affect other areas of life (travel, employment, education). In that regard, the importance of court authorizations, also in the case of bulk data, has already been recognized by the ECtHR (see *Big Brother Watch v. UK*).

[3] See, Cyber Crime Committee, T-CY (2014)17, Rules on obtaining subscriber information, pp.17-20 (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1). See also T-CY (2018)26, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, p. 5-6.

[4] ECtHR, *Benedik v. Slovenia*, a. no. 62357/14, judgment of 24 April 2018.

[5] For example Spanish Constitutional Court, 26/2014 (as answer to the CJEU Melloni decision) or more recently the Italian Constitutional Court, Order 24/2017 and Judgment 115/2018 (as answers to the Taricco case).

b) Offences justifying the issuing of an EPOC(-PR) (Art. 5 and Art. 6)

The Proposal provides for different conditions for an EPOC and an EPOC-PR. While an EPOC-PR may be issued for all criminal offences, there is a distinction with an EPOC. EPOCs addressing subscriber data or access data may be issued for all criminal offences; EPOCs concerning transactional data or content data can be issued, either, for all other criminal offences punishable 'by a custodial sentence of a maximum of at least 3 years', or for those offences listed in existing EU instruments on terrorism, sexual exploitation of children and child pornography, fraud and counterfeiting of non-cash means of payments as well as attacks against information systems. In contrast to the already existing EU instruments in criminal law, however, there is no dual criminality requirement (i.e. the punishable conduct in the issuing state does not need to be considered as a criminal offence also in the executing state) in the proposal, meaning that only the definition of these offences in the issuing state is relevant.

Already in the previous working documents, concerns have been expressed about the extremely limited role for the executing authority envisaged by the Commission proposal. The proposal aims to introduce a 'new dimension' of mutual recognition, by providing for EU-wide enforceability of a national order without any check, neither substantial nor formal, by the executing authority. Considering the existing *acquis* in the field of judicial cooperation, the envisaged reallocation of responsibilities regarding the protection of fundamental rights would be a fundamental novelty,[6] which would dramatically increase the responsibilities of the issuing authority and weaken the protection offered by the executing authority. Apart from doubts regarding what criminal proceedings justify the recourse to such measures (that, among others, may have disruptive effects on the right to privacy), the solution, as proposed by the Commission, is problematic regarding two different aspects.

1) The abandoning of the dual criminality principle

Compared with traditional mutual legal assistance where the principle of dual criminality is applied, the existing EU mutual recognition instruments have already limited the practical relevance of the dual criminal principle. For the offences listed in the EU-catalogue[7], which is supposed to reflect offences, commonly regarded as serious crimes, defined through set of shared values and priorities across Member States, the executing authority can no longer refuse the execution of a foreign decision just because that criminal conduct is not criminalised in the same way in its legal system. However, for offences falling outside of this list, the existing mutual recognition instruments[8] recognise the right that the executing authority '*may*' refuse the exercise of power issued by an authority of another Member State in those cases that are not considered criminal in the executing jurisdiction. Considering the fact that criminal law provisions across the EU are far from being harmonised, such an optional ground for refusal represents a necessary safeguard, in order to ensure full respect of fundamental rights.

Nevertheless, looking at Articles 5 and 6, the current proposal does away with this safeguard.

[6] See the study of the EP Policy Department for Citizens' Rights and Constitutional Affairs by M. Böse, p. 41
[7] See for the list, for example, Article 2(2) of the EAW Framework decision 2002/584/JHA.
[8] See, for example, Article 11 EIO Directive.

Not only would it abandon the typical catalogue of 32 offences included in other mutual recognition instruments, but it would also abolish the dual criminality check for all other offences. Therefore, an EPOC(-PR) could be issued for actions that are criminal in the issuing state, but not criminal in the Member State where the provider sits. This is particularly worrisome concerning areas where a common EU approach is lacking or where positions significantly diverge, e.g. issues such as abortion, euthanasia, religious rights, or limits to freedom of expression.

In order to avoid a situation, in which a service provider might be requested to produce or preserve data about an offence which is not deemed criminal in the Member States where it sits, therefore, it seems necessary to include a closed list of offenses for which an EPOC(-PR) can be issued. Such a list could built on Annex D of the EIO. Considering the structure and functioning of the proposed instrument, the EU legislator should reflect on how to best include such a list. There are two main options: a) It could be a list addressed to the issuing authority, working as an additional condition to issue an EPOC, in order to prevent the issuing authority from issuing an order for offences falling outside the list; b) Similarly to the other EU mutual recognition instruments, and based on the principle of dual criminality, such a list of offences could also be included as a an exception to a newly added optional ground for refusal, allowing the executing authority to refuse an EPOC(-PR) issued for offences not included in the list which is not deemed criminal in its territory.

Another ground for refusal could build on Article 11(1)(h) of the EIO referring to cases where '*the use of the investigative measure ...is restricted under the law of the executing state to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO*'. With this, the executing authorities would systematically be involved in the execution of the order and could thereby exercise their constitutionally guaranteed protective function.