European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

1.4.2019

6th WORKING DOCUMENT (A)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Safeguards and remedies

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel
Co-author: Romeo Franz

Introduction

This Working Document will focus on the safeguards and remedies as foreseen in the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (so-called e-evidence proposal). As such, it will analyse the principle of **notification to the suspect of the request for data** unless a non-disclosure (gag order) is justified on an exceptional basis. Following that, it will examine those safeguards which have to be guaranteed before data is gathered and transferred to the requesting state (so-called ***ex-ante* safeguards**) as well as the remedies which have to be guaranteed after the data has been transferred to the requesting state (so-called ***ex-post* safeguards**). Finally, the working document will elaborate on an **effective oversight and public accountability** mechanism over law enforcement authorities using a possible new instrument on e-evidence.[1]

I. Notification of the data subject

According to Article 11 ("Confidentiality and user information") of the proposed Regulation, addressees shall "take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and where requested by the issuing authority, shall refrain from informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings." (see Art. 11(1)). "Where the issuing authority requested the addressee to refrain from informing the person whose data is being sought, the issuing authority shall inform the person whose data is being sought by the EPOC without undue delay about the data production. This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings." (see Art. 11(2)). "When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17" (see Art. 11(3)).

An important issue as regards the notification of the data subject, which has also been raised by several stakeholders[2], relates to the principle of equality of arms and the adversarial principle that are part of the right to a fair trial (as regards the collection of exculpatory evidence) as outlined in Article 6 of the European Convention on Human Rights.[3] Such a principle, in general, is easily threatened by the secrecy of the preliminary investigation phase and the lack of notification of the data subject about the gathering of personal data. However, prior notification of the suspect or accused is key to ensure an effective exercise of defence rights; namely that, also exculpatory electronic data is preserved (besides incriminating data) and that the suspect or accused may have the possibility to challenge *a priori* the legality of electronic data that may have been obtained illegally or may not be admissible in court.

---

[1] See also Fair Trials International, Consultation Paper, February 2019, p. 4.

[2] Ibid, p. 12: *"In adversarial models, such as in the US, the defence is expected to take on an active role in the preparation of its case, and autonomously gather information and materials. In many legal systems in the EU, broadly described as "inquisitorial", law enforcement authorities are solely responsible for conducting an investigation aimed at establishing the "truth". As such, there are obligations on law enforcement authorities to use investigatory powers to gather all relevant evidence, both incriminatory and exculpatory, and not just evidence which establishes guilt. In reality this is not, however, always the case and even an impartial investigator would be unable to know what evidence might be of use to the accused without consulting them to understand the nature of their defence, which cannot happen where the investigation is secret."*

[3] See Article 6 ECHR case-law, for example, D. Vitkauskas G. Dikov, Council of Europe, Protecting the right to a fair trial under the European Convention on Human Rights, 2012.

The proposed E-evidence Regulation prevents the service provider from informing the person whose data is sought "in order not to obstruct the relevant criminal proceedings". The question arises which situations would actually fall under this formulation. It is a vague wording, which risks encompassing minor obstacles in the proceedings. Yet, as regards the principle of quality of arms any limitation as regards the notification of the data subject (also called "gag orders") must be clearly defined and limited, for example, to cases of serious and clear danger to life, limb or property. In addition, a problem, in general as well as regards confidentiality, might arise as regards the definition of "service providers" from the proposed Regulation and the associated question of differentiating between data controller and data processor:[4] Is the processor also bound by the confidentiality rules and, thus, also inhibited from informing the controller about a received order?[5]

1. Notification of the data subject for production orders (EPOCs):

As regards EPOCs, the proposed Regulation further stipulates that "the issuing authority shall inform the person whose data is being sought by the EPOC without undue delay about the data production" (see Article 11(2)). Yet, the proposal allows that the requesting authority may delay such notification "as long as necessary and proportionate to avoid obstructing criminal proceedings". With this, the proportionality of a delayed notification would be assessed by the issuing authority only. As has already been pointed out in the previous Working Document, it is doubtful whether the issuing authorities could and would actually fulfil these provisions. Existing mutual recognition instruments, such as the European Investigation Order, at least grant some grounds for refusal to the executing state to also question the proportionality[6]. In addition, as regards the issue of necessity, the Regulation, as proposed, gives rise to the concern that such a "gag orders" would be used as a rule, rather than as an exception when strictly required. Since, however, there may be legitimate reasons for secrecy, at least for some types of data and mainly at the beginning of the procedure (i.e. where the procedure is not yet necessarily focused on a particular person), some tensions between the legitimate law enforcement need for secrecy, on one side, and the right to defence and fair trial, on the other side, exist. These might be mitigated by:[7]

• Creating a clear notification regime which strictly limits the exercise of secrecy by law enforcement authorities to exceptional measures,

• Requiring specific justification for the exercise of a gag order by the law enforcement

[4] See Article 2(3) of the e-evidence Regulation. See also Article 4(7) and (8) of the GDPR Regulation 2016/679.
[5] See, EDPB, Opinion 23/2018, stating: *"Hence, the EDPB fears that without limitations to service providers acting as controllers in the sense of the GDPR, and without any specific obligation of the processor to notify the data controller, when addressed with a production or preservation order, data subjects' rights might be circumvented."* (p.10).
[6] The EIO, at least, grants the executing authority some grounds for refusal to also question the proportionality of the request. This holds true with regard to the grounds based on a potential violation of fundamental rights (see e.g. Article 11(1)(f) of Directive 2014/41/EU on the EIO: if 'there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter'), certain threshold/category of offences (see Art. 11(1)(h) of the EIO Directive: if 'the use of the investigative measure indicated in the EIO 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'). as well as with regards to the unavailability of the measure in similar situations in the domestic system of the executing authority (see Art. 10(5) of the EIO Directive).
[7] Fair Trials International, ibid, pp. 5-6.

authorities as well as judicial (court) oversight over the use of gag orders[8]. Here, again, the question regarding the issuing authority for EPOC(-PR) arises, as outlined in the 5th Working Document.

• Clear time limits for the imposition of secrecy (for example, utmost maximum: until indictment);

• Requiring the issuing authorities, when requesting the service provider to refrain from informing the data subject, to submit clear and detailed reasons for the requested non-notification to the service provider;

• Additional notification of the judicial authorities of the Member State where the service provider is established and/or where the person whose data is sought resides,

• A right for service providers, where they are not satisfied by the justifications for a gag order provided by the issuing state, to request further information, including the right to eventually refuse to comply with the order, if doubts about the lawfulness persist; with such a right, issues as regards obligations of service providers vis-à -vis their customers would also be met;

• An obligation for prompt ex-post notification once the legitimate basis for secrecy no longer applies, and, in any case, clearly before the full disclosure of the evidence in the case (regardless of whether the affected person is ultimately prosecuted), with a right for the affected person to challenge the use of secrecy and the legality of the production of the evidence;

• Providing for dissuasive incentives for law enforcement authorities to not misuse this exception, for example, by declaring the evidence obtained inadmissible;

• An explicit obligation for law enforcement authorities requesting electronic data (in the context of secrecy) to generally extend EPOCs and EPOC-PRs to also cover exculpatory evidence or to provide certain rights to the defence side in view of the "equality of arms" principle in criminal procedure.[9]

2. Notification of the data subject for preservation orders (EPOC-PRs)

Serious additional problems arise, as regards the principle of equality of arms, regarding the notification of data subjects in case of preservation orders (EPOC-PR).

As outlined before, if the addressee has been requested to refrain from informing the data subject, the proposed Regulation only foresees that "the issuing authority shall inform the

[8] An independent and impartial court authority is be better suited to assess the need of secrecy v. defence rights than police/prosecutorial authorities. See also CCBE position, 19 October 2018 stating (p. 7) *"The CCBE considers that the imposition of confidentiality restrictions on EPOCs must be subject to the approval of an independent judicial authority and in each case be duly motivated and justified by the issuing authority on the basis of a meaningful and documented assessment"*

[9] In that regard, for example, the EIO can be explicitly used also by the defence. See Article 1(3) EIO Directive stating: *"3. The issuing of an EIO may be requested by a suspected or accused person, or by a lawyer on his behalf, within the framework of applicable defence rights in conformity with national criminal procedure."* Such a provision is lacking in the e-evidence proposal. See also CCBE, ibid, p.7: "*Any proposal for the recovery of e-evidence should not be seen as solely concerned with prosecution... The proposal does not take properly into account the requirement for equality of arms in criminal proceedings, which is a concept recognized by the ECHR in the context of the right to a fair trial."* See also Fair Trials International, Position Paper, May 2018. See also the letter of Fair Trials addressed to the rapporteur, 30 November 2018.

person whose data is being sought by the EPOC without undue delay about the data production" (see Article 11(2)). The proposal does not foresee any obligation of the issuing state to notify the data subject as regards EPOC-PRs. As a consequence, the data subject will never know that his or her data was preserved, in cases where an EPOC-PR is not followed upon by an EPOC. In these cases, the data subject will not have any possibility to challenge the use of secrecy and the legality of the preservation of the evidence. Furthermore, it will not have any access to remedies at all (see below).