**European Parliament**
2014-2019

*Committee on Civil Liberties, Justice and Home Affairs*

13.2.2019

# 3rd WORKING DOCUMENT (A)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) - Execution of EPOC(-PR)s and the role of service providers

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel

Co-author: Daniel Dalton

## Introduction

The third working document on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) will cover the role of service providers in the proposed Regulation.

The system, as proposed by the Commission, envisages a central role for the service providers, by giving the legal representative of the service provider the role of the "addressee" of the European Production/Preservation Order.[1] As such, the contact for and cooperation over an order would, in principle, solely be between the provider and the foreign judicial authority who issued the order. Only in cases where there would be a problem with the execution of such an order the judicial authority of the executing state would also be informed or involved.

In order to properly evaluate this proposed new role for the service providers, the following elements will be further analysed: the internal assessment procedure by the provider, including fundamental rights; the transmission and authentication of European Production/Preservation Orders; the double criminality; the costs; the feasibility and proportionality of obligations for providers; and the liability and sanctions.

## Internal assessment procedure by the provider

The service providers are foreseen, by the Commission proposal, to have a certain narrow margin of assessment when it comes to the two types of orders received from the authorities.

Regarding the production order (EPOC), Article 9 specifies that:

- "*if the addressee cannot comply with its obligation because the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC, the addressee shall inform the issuing authority referred to in the EPOC without undue delay and ask for clarification...*" - Article 9(3) ;
- "*if the addressee cannot comply with its obligation because of force majeure or of de facto impossibility not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the addressee shall inform the issuing authority referred to in the EPOC without undue delay explaining the reasons,* ...". - Article 9(4);
- "*In case the addressee considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive, the addressee shall also inform the competent enforcement authority in the Member State of the addressee. In such cases the competent enforcement authority may seek clarifications from the issuing authority on the European Production Order,*

[1] Article 7 of the proposed Regulation. In case no legal representative has been appointed, does not comply in an emergency case or does not comply with its obligations and there is a serious risk of data loss, it can be also addressed to any establishment of the service provider in the Union.

*either directly or via Eurojust or the European Judicial Network."* - Article 9(5, 2nd part).

Similarly, regarding the preservation orders (EPOC-PR), Article 10 specifies:

- "*if the addressee cannot comply with its obligation because the certificate is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC-PR, the addressee shall inform the issuing authority without undue delay and ask for clarification,...*" - Article 10(4);
- "*If the addressee cannot comply with its obligation because of force majeure, or of de facto impossibility not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the order, it shall contact the issuing authority without undue delay explaining the reasons...*" - Article 10(5);
- However, unlike with the production orders (Article 9(5, 2nd part)), there is no fundamental rights assessment foreseen in Article 10 for preservation orders.

In addition, in the case of non-compliance where a provider has not complied with an EPOC-PR and therefore an enforcement procedure against it has been started as per Article 14, the Commission proposal does foresee further grounds for a provider to oppose the enforcement of an EPOC-PR in the same Article.

Article 14(4) specifies that an addressee may oppose to execute a production order issued/validated by the wrong authority, or one issued for another offence than those listed in Article 5(4). The service provider may also cite force majeure/manifest errors, data not stored by or on behalf of the service provider at the time of the receipt of EPOC, the addressee not being covered by the Regulation, or for the EPOC manifestly violating the Charter or being manifestly abusive.

When it comes to preservation orders, Article 14(5) stipulates that an addressee may oppose to execute one issued/validated by the wrong authority, for force majeure/manifest errors, for data not being stored by or on behalf of the service provider at the time of receipt of EPOC-PR, for the addressee not being covered by the Regulation, or for the order manifestly violating the Charter or being manifestly abusive. With this, there seems to be an inconsistency in the Commission proposal; whereas Article 10 does not foresee a fundamental rights assessment regarding the preservation orders (unlike for the production orders), such a ground is mentioned for the preservation orders in Article 14(5)(e).[2]

Finally, Articles 15 and 16 of the proposed Regulation foresee the possibility to trigger a specific review procedure in the issuing state[3]. If the addressee considers that compliance with an EPOC would result in conflicting obligations based on fundamental rights or fundamental interests of a third country (Article 15), or in case of conflicting obligations based on other

[2] The Council, in its General Approach, fully deleted such an assessment, even in the enforcement procedure of Article 14.

[3] However, there could be a situation where another Member State is involved in case the legal representative of a third country service provider is in another Member State. In that case also international relationships between that Member State (state of enforcement) and a third country could be at stake. However, it is not foreseen that a legal remedy is possible in such case in the Members State of enforcement ("executing" State).

grounds (Article 16), a review procedure may be possible.[4]

In that regard, the Commission proposal gives a certain leeway to the service provider regarding the assessment of received orders. As expressed in the LIBE hearing[5] and based on information gathered from providers, some providers already conduct such an assessment. According to those service providers, they do not execute manifestly erroneous, arbitrary or unspecified requests (for example, pure "fishing expeditions") by law enforcement authorities. Such a procedure is widely accepted as having an added value regarding the efficiency of orders. Moreover, providers appreciate the possibility not to execute orders that are manifestly erroneous, arbitrary or unspecified, as they are responsible for the protection and privacy of the data of their customers, it is the core of their business model and the source of their customers' trust in them. [6]

However, regarding the European Production and Preservation Order Certificate, the Regulation proposal stipulates, in Article 8(3) and (4), that providers will only receive very limited information regarding the specific case to which an order is linked.[7] Thus, it is not clear how providers could actually be in a position to make a real assessment, especially with regards to the fundamental rights assessment of production orders.

Moreover, notwithstanding the fact that most parties welcome an assessment procedure for

[4] As regards Article 15, the procedure was foreseen in the case of conflict with a law of a third country in connection with fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence. A particular procedure is foreseen whereby the court informs the other state which has a certain deadline to oppose. In comparison, Article 16 is foreseen for all other cases, whereby the court does not inform the third country authorities in case of conflict and takes an autonomous decision based on certain proscribed criteria. The Council in its general approach deleted Article 15.

[5] The Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament organised a public hearing in Brussels on 27 November 2018 on "Electronic evidence in criminal matters"

[6] See, contribution of Vodafone, EP Hearing on e-evidence, 27 November 2018, http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEE-LIBE. However, the Council general approach seems to narrow such a possibility even more. See, Microsoft's Response to the Council Position on the Proposed e-evidence Regulation, January 2019, p. 5 ("*The Council text does not give service providers any right or mechanism by which to raise concerns about the legality of orders they receive under the Regulation. Empowering service providers to raise such concerns is critical, because, in some cases, only service providers will have the ability to identify demands that are overly broad or inappropriate for other reasons."*). This is connected also with the proportionality issue as further stated by Microsoft *("Take, for example, the case of law enforcement authority investigating a crime involving certain employees of "Acme Company". LEA might issue an EPO seeking all emails sent from the "Acmecomapny.com" domain without realizing that the company has thousands of employees who send emails from that domain..."*).

[7] See Article 7 of the proposed Regulation. A very limited number of information is provided - see Article 5(5) on the EPOC and 6(3) of the proposed Regulation on the EPOC-PR, namely information on: - the issuing and, where applicable, the validating authority; - the addressee of the order; - the affected person(s); - the data category (subscriber data, access data, transactional data or content data); - if applicable, the time range requested; - the applicable provisions of the criminal law of the issuing State; - the grounds for the necessity and proportionality of the measure; and, in addition, for production orders also - in case of emergency or request for earlier disclosure, the reasons for it; and - confirmation that in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate. However, as regards information on necessity and proportionality, it is not clear how it relates with Article 8(4) stating: *"The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included."*

service providers with regard to errors, force majeure and data protection and contract obligations of the service providers, it has to be clarified if a fully-fledged fundamental rights assessment (as foreseen in Article 9(5, 2nd part) as well as Article 14 (4)(f) and (5)(e)) can and should be outsourced to them. By outsourcing such an assessment obligation to the providers, the authorities of the state of enforcement, in principle, would no longer get any notice of the production or preservation and thus would have no possibility to stop the order. As a result, the authorities of the state of enforcement would basically lose any sovereign prerogatives on data, or on guaranteeing fundamental rights on their territory. 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.[8]

The importance of sovereign prerogatives, especially the privacy rights, seems even more crucial in reference to the current patchwork of data retention laws in the EU,[9] including the unclear legal situation of validity of national data retention provisions[10], as well as the unsolved issue of the authorising authority for dynamic IP addresses (different approaches in different Member States).[11]

---

[8] See, in that regard also obligations by Article 1 ECHR on the Contracting Parties to the Convention - See CoE, Guide on Article 1 ECHR, Obligation to respect human rights, Concepts of "jurisdiction" and imputability, 2018 (https://www.echr.coe.int/Documents/Guide_Art_1_ENG.pdf). See, also *Jaloud v. Netherlands* (GC), a. no. 47708/08: *"143. Furthermore, the fact of executing a decision or an order given by an authority of a foreign State is not in itself sufficient to relieve a Contracting State of the obligations which it has taken upon itself under the Convention (see, mutatis mutandis, Pellegrini v. Italy, no. 30882/96, § 40, ECHR 2001-VIII, and K. v. Italy, no. 38805/97, § 21, ECHR 2004-VIII)."* See, also ECtHR, *Bosphorus et al. v. Ireland*, a. no. 45036/98 (EU fundamental rights protection equivalence); *M.S.S. v. Belgium and Greece* (GC), a. no. 30696/09 (disapplication of the Bosphorus presumption); as well as *Avotinš v. Latvia*, a. no. 17502/07 (limits to mutual recognition and trust). The issue has been also raised by ECHR Judge Prof. Dr. Bošnjak, e-evidence EP hearing, 27 November 2018 (especially 16.55-16.58 explicitly on the issue - *"As far as the law of the enforcing state is concerned it seems to be of no relevance according to the existing proposal. From the point of view of the Convention this can create a problem because the High Contracting Parties to the ECHR, including all 28 MS EU, are responsible for protection of human rights on the territory under its jurisdiction. ..They have to put a place a regulatory framework and also guarantee legal, if no judicial, protection in particular cases... If the authorities of the enforcing state are faced with a complaint that the protection of Convention right has been manifestly deficient and this cannot be remedied by EU law, they cannot refrain from examining the complaint on the ground the they are just applying EU law. This has clearly bee stated in the judgement of Avotinš v. Latvia... The proposal, as it is before you, crates a rather unique situation from the point of ECHR jurisprudence. The interferences with Article 8 are without any involvement of the authorities of the enforcing state. I wonder, if this is in line with the ECHR. There might be a legitimate expectation that the law of the enforcing state would apply in each and every particular situation. This would affect the assessment of lawfulness..."*).
See under http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEE-LIBE.

[9] After the EU Court of Justice decision in Digital Ireland.

[10] EU Court of Justice, joint cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others. See, also Cable Europe Position paper, p. 3 ("However, the status of the data retention obligations currently in place at national level - following the invalidation of the EU Data Retention Directive by the CJEU - is unclear... The service provider may well not hold the data requested by the issuing authority."). See also ETNO position paper stating: "It is important to stress the difficulties to clearly distinguish in practice between "access" and "transactional" data... it is necessary to have to have judicial oversight for all requests, related to a determined list of offences and for all data categories..."

[11] The Commission proposal with the introduction of a new special category of "access data" seems does not solve the issue of the different national authorities, especially as regards the trend of court authorisation for such data. See, for example Cable Europe Position Paper, 11 October 2018 9"Issuing an order should be a genuine

Apart from the problem of outsourcing sovereign prerogatives to private parties, it is highly questionable to put the service providers in the position of adjudicating on citizens' fundamental rights, which, they themselves argue, they can and do not want to fulfil.[12] Furthermore, they must be able to operate on clear legal rules, in regard to other EU Member States, as well as all third states. The question therefore is how far the Commission proposal provides for such legal clarity or necessary guarantees due to the lack of the final arbitration of the judicial authority of the State of enforcement.

The remaining question therefore is whether a stronger involvement of the authority of the state of enforcement (e.g. in form of a notification of such authority, including a deadline for a meaningful reaction or objection, where necessary) (similar to Article 31 EIO) would bring clarity. Such a notification regime could, on one hand, uphold sovereign prerogatives, and, on the other, provide additional guarantees and legal certainty to the providers (including relieving them from liability issues).[13]

---

court decision"). See also, the issue analysed by the CoE Cyber Crime Committee, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments, T-CY (2018)26, 25 October 2018 (see in detail EP Working document 2 on the issue). See also Microsoft Response to the Council Position on the proposed e-evidence Regulation, January 2019, stating, inter alia, that "low enforcement demands for content and other sensitive data must be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing.

[12] See, for example, the ETNO (European Telecommunications Network Operators' Association) Position paper (supported, for example, by KPN) on improving cross-border access to electronic evidence in criminal matters ("The role that the proposal foresees for the service providers seems unrealistic. Telecom operators are not in a position to guarantee, for example, that the order does not violate the Charter. Similarly, the authenticity and legal validity of the orders... should not be a responsibility of the operators... Therefore, industry thus cannot replace judicial authorities in their key role of assessing compliance of an EPO").

[13] The Council deleted any autonomy in the assessment of the service providers and included a notification but only in if the person concerned is not residing in its territory and only for content data (not other categories) without a possibility to stop the transfer of data. The State of enforcement can only in limited enumerated cases (the data requested is protected by immunities and privileges granted under the law of the enforcing State, or is subject in that Member State to rules relating to freedom of press and freedom of expression, or to fundamental interests of the enforcing State such as national security and defence). However, the issuing authority shall take these circumstances into account in the same way as if they were provided for under its national law. See Article 7a of the Council general approach, doc. 15020/18. In new Article 12a also a possibility by the issuing state of taking in case of transactional (traffic) data such info "into account in the same way as if they were provided for under their national law". However, it is not clear how the issue would be raised if the State of enforcement is never notified and not even aware. The issue was raised, for example, by Microsoft (Paper on Council general approach, January 2019) stating *"That approach makes little sense... Indeed, given how many service providers host data in Ireland, Irish authorities could be inundated with notices under the Council proposal, but often will have no way to evaluate whether the data at issue is subject to legal protection. Proposed position: Require issuing authorities to notify affected Member States. The Regulation should require the issuing authority to notify EPOs to the Member State where the person targeted by the order resides. This State will be in the best position to identify any applicable protections and will have the strongest interest in defending these protections. This solution should not be unduly burdensome: in Microsoft's experience, only around 7% of law enforcement authorities demands for user data involve targets located in a different Member State."* See also Bitkom Position paper stating *"Beyond notifying impacted users and customers, the Regulation should make it clear that companies may notify the central authority in any Member state whose sovereign interests are implicated by the request."* A similar position of the necessity of the involvement of a public authority in the State of enforcement was also raised by KPN ("The legitimacy of orders cannot (and should not) be materially judged by private service providers"). The same expressed by EuroISPA, June 2018 Position paper ("*We criticise the further privatisation of law enforcement by this proposal"*).

**Transmission and authentication of EPOCs and EPOC-PRs**

The EPOC(-PR) shall be transmitted directly from the issuing authority in one Member State to the provider (legal representative) in another Member State (or the representative for a third country provider operating in the EU) through a standardised certificate.[14]
The proposed Regulation is rather vague on the actual modalities of the transmission and only states that the EPOC(-PR) "*shall be directly transmitted by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity*".

Where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities, the issuing authority may also choose to transmit the Certificate via these channels.[15] Consequently, there is no common, centralised or secure transmission gateway foreseen in the instrument and the issue is left open to Member States and providers, despite the instrument being nominally a Regulation.[16] Instead, the Commission states in the accompanying statement to the proposal that the use of already existing platforms shall not be prevented by the Regulation, as it offers many advantages, including the possibility of an easy authentication and a secure transmission of the data.

However, it should be mentioned that these platforms would have to allow for the submission of the EPOC and the EPOC-PR in the format as provided for in Annexes I and II, without requesting additional data pertaining to the Order. Therefore this inevitably means that such platforms would have to be adjusted and it is not clear who would bear the costs for that. The Commission also refers to existing centralised EU platforms, such as e-Codex[17] and

[14] See Article 7 of the proposed Regulation. A very limited number of information is provided - see Article 5(5) on the EPOC and 6(3) of the proposed Regulation on the EPOC-PR, namely information on: - the issuing and, where applicable, the validating authority; - the addressee of the order; - the affected person(s); - the data category (subscriber data, access data, transactional data or content data); - if applicable, the time range requested; - the applicable provisions of the criminal law of the issuing State; - the grounds for the necessity and proportionality of the measure; and, in addition, for production orders also - in case of emergency or request for earlier disclosure, the reasons for it; and - confirmation that in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate. However, as regards information on necessity and proportionality, it is not clear how it relates with Article 8(4) stating: *"The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included."*

[15] See Article 8 of the proposed Regulation.

[16] This was, for example, criticised by ETNO: *"It would be crucial to build a centralized secure transmission channel, a sort of unique platform: - receiving the request from law enforcement authorities of the issuing Member State; - checking the validity of the request... via a competent judicial authority in the enforcing state; and - forwarding the requests to the service provider... The platform will then ensure that the request is authentic, adequate and can be met..."* Specifically, e-Codex is mentioned: *"For that, it should be necessary that the e-Codex Regulation and its implementation be ready by the time the -evidence Regulation becomes applicable. In a transitional phase before the secure platform is established and operational, it could be important to constitute a judicial single point of contact in each Member State, charged to receive and validate transmission of the other Member State."* Similar Vodafone, EP Hearing on e-evidence, 27 November 2018, http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEE-LIBE.

[17] e-CODEX" is an IT system for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. It operates as a decentralised network of access points, interlinking national and

SIRIUS[18], and raises the theoretical possibility to enlarge them to cover service providers, yet, without any fixed timetable or firm commitment of doing so.[19] Consequently, the question is how will the provider actually know that the EPOC(-PR) received is from an authentic foreign judicial authority and that it is not a case of "identity theft" or of a fraudulent exercise. Similar problems are to be expected with regard to the transmission of the requested data, from the service provider back to the issuing authority in another Member State. With regards to the sensitivity of the data, on the one hand, as well as the potential size of the data files, on the other hand, service providers and Member States should be able to rely on secure ways of transmission of the data.

Thus, if the proposed e-evidence system should be feasible, the precondition must be that a secure communication channel is put in place, providing at the same time a guarantee to the provider regarding the authenticity of the request, as well as the security of the channel to transmit the requested data. In view of the Commission intended deadline for the date of application of the proposed Regulation (6 months after its entry into force), it is clear that the Commission did neither plan to have a common system as part of the proposal nor to have it operational by the entry into force.

With regards to the Commission reference to e-Codex and Sirius, one has to take into account that both projects are at an 'experimental' or 'test' phase with no full-fledged common operational platform in place. However, various Member States are already using e-CODEX to support cross border legal procedures both in civil and criminal matters, for example for the exchange of requests for mutual legal assistance between public prosecutors. Taking into account the issues raised concerning user authentication and secure data transmission, the

---

European IT systems to one another. Specific software is required to establish an e-CODEX access point. The e-CODEX system has been developed in the context of the Digital Single Market by a group of Member States with the help of EU grants - it was developed under the Competitiveness and Innovation Framework Programme (CIP) ICT Policy Support Programme by a consortium of Member States. It was intended for civil and criminal law. The e-Codex platform would be used also by e-evidence (MLA, EIO and potentially e-evidence). In that context a grant was given to the Evidence2e-Codex project (10 Member States and 21 partners, 2018-2019). Implementing cooperation with providers was only part of the expected results as it focuses on EIO and MLA requests in connection with e -evidence. However, the programme is at an initial/test phase and a fully operational platform does not exist yet. At a pre-stage the Evidence project has been conducted running from 2014-2016 (participation by Italy, Netherlands, France, Germany, Malta, Belgium and Bulgaria). The main findings of the mentioned project were: - there is no comprehensive legal framework as regards electronic evidence collection, preservation, storage, use and exchange; - in spite of this lack of comprehensive legal framework electronic evidence is increasingly key evidence in criminal procedures; - the lack of this comprehensive legal framework leaves LEAs to operate in a patchwork of solutions, be it legal, data protection, enforcement or technical solutions; - the stakeholders involved feel a need for the creation of certification and professionalisation of the persons involved in and environments where electronic evidence is persevered, stored, analysed and exchanged (see evidenceproject.eu).

Also Interpol has an e-MLA expert Working Group. However, it has to be taken into account that Interpol comprises a set of very different states, not only EU Member States. A EU e-evidence platform would have to fully comply with EU data protection standards.

[18] SIRIUS is a secure web platform for law enforcement professionals launched by Europol in 2017. It allows to share knowledge, best practices and expertise in the field of internet-facilitated crime investigations by investigators, with a special focus on counter-terrorism. It also addresses other challenges in criminal investigations, such as streamlining the requests to online service providers, and improving the quality of the responsive record.

19 see p. 18 of the Explanatory Memorandum of the proposed Regulation: "consideration should be given to a possible expansion of the e-Codex and SIRIUS platforms to include a secure connection to service providers for the purposes of the transmission of the EPOC and EPOC-PR and, where appropriate, responses from the service providers"

Commission should .assess possibilities for improved transmission security between service providers and law enforcement authorities