European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

13.2.2019

3rd WORKING DOCUMENT (B)

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

Costs

The proposed Regulation also envisages a new system for reimbursement of costs, yet with rather unclear rules regarding the providers. Article 12 of the proposed Regulation states that the service providers "*may claim reimbursement of their costs by the issuing State, if this is provided by the national law of the issuing State for domestic orders in similar situations, in accordance with these national provisions*".[1] Therefore, the providers would need to know the national reimbursement regime of all EU Member States participating in the Regulation, in order to correctly claim any costs from the issuing State. Furthermore, in several Member States, the cost reimbursement system covers capital investments (Capex) by service providers, for example to put in place appropriate specific secure infrastructure for law enforcement disclosures, which could not be replicated, on a per-order basis, for service providers outside of that Member State. Especially when it comes to the small and medium sized enterprises, this is impossible. It is clear though, that the costs for the execution of EPOC(-PR) cannot simply be shifted to operators, especially on the legal basis of Article 82 TFEU, [2] all the more because the providers might already face costs in the preparation of the e-evidence instrument, specifically when appointing the legal representative and additional staff for the execution of EPOC(-PR)s, purchasing of secure transmission channels for data, etc.

In comparison, the current system of mutual recognition in EU criminal law, especially the gathering of evidence, is based on a system whereby the costs are, as a general rule, covered by the executing state, with the exemption of extraordinary costs or based on some specific provisions for specific measures.[3] Based on such a system, the provider has the guarantee to

---

[1] The Council, in its General Approach, tried to improve the provision by adding "Member States shall inform the Commission about rules for reimbursement who shall make them public". See Council general approach, doc. 15020/18.

[2] See, for example, the ETNO position stating "Compliance with the new provisions will require substantial capital and operational costs by telecom operators..."). Also Vodafone called for an EU reimbursement scheme and substantial costs. 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.

[3] See Article 21 of Directive (EIO) 2014/41/EU as regards the general principle, as well as specific provisions on some measures, for example on temporary transfer of persons in custody (Articles 22 and 23 EIO), on interception of telecommunications with technical assistance of another Member State (Article 31 EIO). In addition, Recital 23 EIO states: *"The expenses incurred in the territory of the executing State for the execution of an EIO should be borne exclusively by that State. This arrangement complies with the general principle of mutual recognition. However, the execution of an EIO may incur exceptionally high costs on the executing State. Such exceptionally high costs may, for example, be complex experts' opinions or extensive police operations or surveillance activities over a long period of time. This should not impede the execution of the EIO and the issuing and executing authorities should seek to establish which costs are to be considered as exceptionally high. The issue of costs might become subject to consultations between the issuing State and the executing State and they are recommended to resolve this issue during the consultations stage. As a last resort, the issuing authority may decide to withdraw the EIO or to maintain it, and the part of the costs which are estimated exceptionally high by the executing State and absolutely necessary in the course of the proceedings, should be covered by the issuing State. The given mechanism should not constitute an additional ground for refusal, and in any event should not be abused in a way to delay or impede the execution of the EIO."* In that regard the proposal diverts from the mutual recognition principle as well as from the general MLA principle on costs (see Article 21 CoE MLA Convention with the exception of interceptions - see Article 21 EU MLA Convention). See also Article 30 EAW ("Expenses incurred in the territory of the executing Member State for the execution of a European arrest warrant shall be borne by that Member State."); etc.

be reimbursed. This is important for private entities, especially small and medium sized enterprises, who must have foreseeability in their expenses and costs.

Consequently, it seems necessary to envisage a reimbursement regime, which is based on or similar to the current system of mutual recognition in EU criminal law, whereby the costs, in principle, are born by the executing state where the provider or representative sits.[4] This, again, raises the question about the possible involvement of the judicial authorities of the executing state.

Feasibility of obligations for providers and the issue of dual criminality

The proposed Regulation (Article 9(1) and 9(2)) envisages a deadline of 10 days and in urgent cases 6 hours for providers' to transmit the requested data to the issuing authority. Even though other EU criminal law instruments, e.g. those related to the field of cyber-crime, also foresee such an emergency procedure, they only stipulate a reaction time of 8 hours for 24/7 contact points. Moreover, within this time, not necessarily the requested information but only some basic information has to be delivered.[5] Therefore, the envisaged time-limit of 6 hours for service providers seems extremely ambitious, if not impossible, especially when it comes to small and medium-sized service providers or third country service providers, operating in different time-zones.[6]

Apart from the question on whether the proposed deadlines are feasible, they should also be reassessed concerning fundamental rights guarantees. Since the proposed Regulation would abolish the dual criminality check for all offences and would also not include the typical catalogue of 32 offences from past mutual recognition instruments,[7] a request could concern actions that are not even criminal in the State where the provider sits. This is particularly worrisome concerning crimes, where a common EU approach is lacking or significantly diverges (issues such as abortion, euthanasia, religious rights, or limits of freedom of expression where States have a 'margin of appreciation').[8] The Regulation could include a clear list of offenses covered, for example building on Annex D of the EIO Directive.

---

[4] See, for example, the comments of Cable Europe, Position Paper on -evidence, 11 October 2018, p. 3 *("...it should at least be possible for a service provider to claim reimbursement if such possibility exists in the Member State where the order is addresses. Further, it is particularly important that the compensation is not claimed abroad, which would be particularly burdensome in case of large number of requests..."*).

[5] See, for example, Article 13(1) of Directive 2013/40/EU on attacks against information systems - *"Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer."*

[6] See, for example, the Bitkom comment (Position Paper on e-evidence) - *"With regard to the currently discussed 6-hour timeline, Bitkom would like to raise the issue that this would effectively lead to a 24/7 duty of all providers. This would heavily burden all providers and will especially pose challenges for smaller providers with less financial and personal resources."* 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. Also on the unclear provisions how the data has to be delivered.

[7] It has been shown in WD 2 that this is already the case for subscriber data, including IP addresses, in the EIO.

[8] This are categories whereby by the ECHR a certain margin of appreciation exists, meaning that divergences are allowed by the ECHR system and the EU neither has common standards. See, for example, ECtHR, *A, B, and C v. Ireland*, a. no. 25579/05, as regards Article 8; *S.A.S. v. France,* a. no. 43835/11, as regards Article 9. See older, for example, ECtHR, *Handyside v United Kingdom*, a. no. 5493/72, on Article 10; see also CoE, Margin of Appreciation, 2000, https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf.

Consideration should be given so that the criminal offence being investigated by the authority of the issuing Member State is also criminal offense in the Member State where the service was accessed. Having this sensitivity in mind, as well as the rather short deadlines, the question of a potential notification of the judicial authorities in the enforcement state needs to be raised again, as also mentioned by several providers[9] and legal experts[10]. Such an inclusion could provide the service providers the legal certainty they have requested.

Liability and sanctions

Article 13 of the proposed Regulation stipulates that the "*Member States shall lay down the rules on pecuniary sanctions applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 of this Regulation and shall take all necessary measures to ensure that they are implemented. The pecuniary sanctions provided for shall be effective, proportionate and dissuasive*."

The question of liability of providers is closely connected with the question of legal certainty of the proposed system. Having said that, the envisaged e-evidence system, on the one hand, as well as already existing legal obligation of service providers, on the other, such as national criminal rules for unauthorised disclosure or EU data protection rules (Regulation (EU) 2016/679), seem to put service providers in a legal limbo. In such a limbo, service providers, acting in good faith in compliance with an EPOC(-PR) might face risks of sanctions due to unlawful collection of customers' personal data in contradiction with data protection laws. This legal uncertainty is further exacerbated by the fact that both systems foresee substantial penalties in the case of non-compliance.[11]

Only Recital 46 makes a reference to this uncertainty by stating that "*Notwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR*." It is, however, doubtful whether such a reference in a recital would allow for enough legal certainty for the service providers in the proposed instrument.[12]

Having addressed the question of the legal basis and the choice of the legal instrument already in the second Working Document, it is worthy to mention it also here. The proposal is based on Article 82(1) TFEU solely and no sanctions were ever proscribed under the mentioned article as the sole legal basis.[13] Furthermore, despite the fact that the Commission proposal is a Regulation, the Commission intends to leave the sanctions to be determined by the Member States. This, again, shows the 'hybrid' nature of the instrument, namely not being a real

---

[9] See, for example, EuroISPA Position paper on e-evidence *("Clarity is needed regarding the principles of double criminality... This would serve to ensure legal clarity for ISPs in complying with production orders.")*

[10] See the statement of ECHR Judge Prof. Dr. Bošnjak referring to problems with the criteria of foreseeability of the intrusion into Article 8, EP hearing on e-evidence, 27 November 2018, http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEE-LIBE.

[11] See Article 13 of the proposed Regulation, as well as Article 83 of Regulation (EU) 2016/679

[12] See also 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.
In this regard, the secrecy (confidentiality) provision of Article 11 has been heavily criticised by the providers who argue that service providers should also be permitted to notify the users and customers affected by the request with secrecy only being the exception.

[13] Sanctions (penalties) can be find under the joint legal basis of Article 82(1) and 87(1) in the PNR Directive.

Regulation having direct effect, but still depending on substantial references to national law provisions.[14] The Council General Approach, by contrast, stipulates that "*Member States shall ensure that pecuniary sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed"*.

Where the Commission sanction system is based on the ancillary powers notion, the Council addition would clearly go beyond that. This, again, would raise issues in reference to proportionality of such a system, the nature of such penalties[15] and, consequently, about the legal basis.[16]

Conclusions

In light of increased cross border data flows and the volatility of electronic data, the EP negotiating team recognise the current challenges law enforcement authorities face and that additional measures may be necessary to tackle crime across the EU quicker and more efficiently, while offering legal certainty for providers and protecting fundamental rights. With regard to the role of service providers, the following can be concluded:

- Some of the main issues of the proposed e-evidence system revolve around user authentication and secure data transmission, in order to allow for adequate authentication procedures for the service providers as well as secure channels of data transmission. Taking into account these issues, the Commission should assess possibilities for improved transmission security between service providers and law enforcement authorities.
- Providers, especially small and medium-sized ones, need clear and foreseeable procedures regarding costs and cost reimbursement. A reimbursement regime similar to the current system under mutual recognition in EU criminal law, might be necessary.

- Regarding the importance of sovereign prerogatives, especially those concerning privacy rights, there are legal and practical limits to which public prerogatives and assessments can lawfully be shifted to private service providers.

---

[14] See more on that in EP 2nd Working document.

[15] See, for example, Court of Justice EU, Joined Cases C-596/16 and C-597/16*, Enzo Di Puma***:**
"38. In that regard, it is apparent from the order for reference that the acts of which Mr Di Puma and Mr Zecca are accused in the context of the proceedings for an administrative fine at issue in the main proceedings are the same as those on the basis of which criminal proceedings were brought against them before the Tribunale di Milano (District Court, Milan). Moreover, the administrative fines at issue in the main proceedings can, according to the information in the case file before the Court, reach, in accordance with Article 187a of the TUF, an amount 10 times greater than the proceeds or profit derived from the offence. It thus appears that they are punitive in character and present a high degree of severity and, therefore, are criminal in nature for the purposes of Article 50 of the Charter (see, to that effect, judgment of 20 March 2018, Garlsson Real Estate, C-537/16, EU:C:2018:193, paragraphs 34 and 35), which it is however for the referring court to determine."

[16] The Council general approach mimics the GDP Regulation. However, there such provisions are under the notion of administrative fines (Article 83 GDPR) and is not part of Article 84 (Penalties). See, for example, also the criticism of Microsoft ("This provision could lead to results that are inconsistent with the EU Treaties because it authorises Member States to impose sanctions that are vastly disproportionate to the Regulation's legitimate aims") referring to Court of Justice case-law (case C-375/96, Galileo Zaninotto v. Ispettorato Centrale. A "criminal" nature of the mentioned penalties would raise the issue of Article 49 of the Charter as regards proportionality as well as defence rights (per analogy to competition case-law proceedings). See, in that regard also Court of Justice case-law under https://fra.europa.eu/en/charterpedia/article/49-principles-legality-and-proportionality-criminal-offences-and-penalties.

- Service providers need full legal certainty when it comes to their obligations and liability and should not be left in a legal limbo between law enforcement/judicial orders, data protection obligations and third country laws. The proposed Regulation, however, seems to unfortunately exacerbate the legal uncertainty for the service providers.

- The possibility of a stronger involvement of the authority of the state of enforcement (e.g. in form of a notification of the authority, including a deadline for a meaningful reaction (and objection, if necessary)) should be further explored, as also suggested not only by the providers but also by eight Member States[17].

[17] See the Joined Letter of eight Member States (Netherlands, Germany, Czech Republic, Finland, Latvia, Sweden, Hungary and the Hellenic Republic), sent to the Austrian Presidency on 20th November 2018, in which "great concern" regarding the compromise proposals for the Council General Approach have been outlined.