European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

7.12.2018

WORKING DOCUMENT

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters - Introduction and overall assessment of issues (2018/0108 (COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel

Introduction

This document sets out the background to the legislative proposal on the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final - 2018/0108 (COD)). Its main objective is to introduce a number of questions for discussion that will be followed-up by topical working documents. The rapporteur thereby seeks to provide input in view of the further phases on the proposed legislative file in the European Parliament.

Background

The Commission proposed, on 17 April 2018, the so-called "e-evidence package", namely:

- the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final - 2018/0108 (COD));
- and an accompanying proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226 final - 2018/0107 (COD)).

The aim of these new instruments is to replace the classical instruments of cross-border cooperation in criminal law (either mutual legal assistance (MLA) or mutual recognition between judicial authorities) with a new approach, whereby cooperation as regards e-evidence would be based on direct orders by an issuing authority in one Member State to a service provider, or its legal representative, in another Member State.[1]

The Regulation proposes to create two new instruments:

- a European Production Order (EPOC), allowing a judicial authority in one Member State to directly request electronic evidence (including content data) from a service provider, or its legal representative, in another Member State (without the other state being informed, or being a part of the procedure). The service provider would be obliged to deliver the requested data within 10 days or even within 6 hours in cases of emergency:

- a European Preservation Order (EPOC-PR), allowing a judicial authority in one Member State to request that a service provider, or its legal representative, in another Member State preserves specific data for a duration of 60 days (with a possibility of a further request), without the other Member State being informed or being a part of the procedure. The preservation order may subsequently be followed up by a request to produce this preserved data, via mutual legal assistance, a European Investigation Order or a European Production Order.

The Directive proposes to supplement the framework provided by the Regulation, by introducing the requirement of nominating a representative for service providers offering services in the EU.

[1] The initial purpose of the Commission proposal was to cover on-going criminal procedures. However, the current text of the Council general approach wants to broaden it to "the execution of custodial sentences or detention orders that were not rendered in absentia in the case the convict absconded from justice" (see Article 3, Council, doc. 14351/1/18, 30 November 2018. In addition, the title of the proposal is broader referring to "criminal matters".

Notwithstanding the general need for a faster, but also more transparent, access to e-evidence, given its volatile nature, scholars, legal experts, fundamental rights and data protection institutions and stakeholders, as well as affected parties like service providers (both the bigger players, but also the SMEs), practitioners and lawyers have raised a number of serious legal concerns, among others, relating to[1]:

- questions regarding the interpretation of Article 82 TFEU and the relationship between mutual recognition and fundamental rights, especially with regards to the ongoing lack of harmonisation of Member States' criminal law and national (constitutional) standards;

- proportionality;

- the question of dual criminality;

- the added value of the proposed instrument, considering that the existing European Investigation Order covers the same issues, was only transposed in 2017 and has not been evaluated yet[2];

- questions regarding the current MLA and mutual recognition systems;

- the relationship of the proposed instrument to the provisions of the Council of Europe Budapest Cybercrime Convention[3], especially with regards to the ongoing debate on its reform;

- questions regarding the extra-territorial application of law;

- questions regarding the privatisation of criminal law, by handing over the assessment of legality and fundamental rights to the private providers and not a state authority;

- data protection implications and compatibility with the EU data protection system as well as the Charter and ECHR case-law, in particular regarding the right to privacy (including the implication of the new data categories introduced in the proposal and the question of the competent/appropriate authority to authorise a production/preservation order for these types

[1] A whole variety of opinions has been issues, inter alia, by the European Data Protection Board (EDPB), https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf, the Council of Bars and Law Societies of Europe (CCBE) (https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf), EuroIspa (http://www.euroispa.org/e-evidence-euroispa-adopts-position-paper/), Electronic Privacy Information Center - EPIC (https://epic.org/2018/11/at-european-parliament-epic-pr.html), Bundesrechtsantwaltskammer -BRAK (https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-europa/2018/september/stellungnahme-der-brak-2018-28.pdf), CEPS (https://www.ceps.eu/publications/cross-border-access-electronic-data-through-judicial-cooperation-criminal-matters), etc. In addition, critical opinions were expressed by a variety of other actors, like Member States (see the letter of eight justice ministers to the Council presidency of 20 November 2018), - telecommunication providers, like KPN, Vodafone, German Association of Judges, an ECHR judge, etc. See also EP LIBE hearing of 27 November 2018 (http://www.europarl.europa.eu/committees/en/libe/events-hearings.html?id=20181112CHE05283).

[2] See, EJN table on transposition under https://www.ejn-crimjust.europa.eu/ejn/NewsDetail.aspx?Id=547.

[3] CoE, ETS 185, especially as regards understanding Article 18, and debates about a new additional protocol.

of data);

- procedural safeguards (including the right to information and the right to an effective remedy);

- practical questions regarding the execution of an order (information provided in the certificate, deadlines etc.).

General remarks on some specific issues

Extra-territorial application of law and the principle of mutual recognition

The proposal introduces the concept of extra-territorial application of law. As a result, the authorities, on whose territory a provider has been requested to produce or preserve data by an authority of another Member State, will not be aware about the request and, thus, will not have the possibility to object to it, even if the offence concerned does not amount to a criminal offence on the territory concerned Aside from the fact that the Member State concerned, with this, risks not to become aware of developments or new trends regarding criminal activities on its territory, basically any rules, including constitutional protections, of the Member State concerned and any prerogatives of its judicial bodies on its territory cease to apply. By contrast, only the service provider of the concerned Member State (or the legal representative therein) will be aware of the order it will be only up to him to check the order on manifest errors, manifest abuses or violations of the Charter.[1]

For this purpose, the Commission interprets Article 82(1) TFEU, serving as the legal basis for the proposed instrument, in a very broad legal manner, namely not as judicial cooperation between judicial authorities but as direct orders directed towards private providers in another Member State. With this broad interpretation, the proposal enters into the legal debate about the nature of "principle of mutual recognition" in criminal matters.
Even though, based on the Treaty and taking into account the principle of conferral of powers (Article 5 TEU), several powers have been conferred from the Member States to the Union based on its 'supranational' structure, a very strict interpretation of legality continues to apply in criminal law. Past mutual recognition instruments, mainly the European Arrest Warrant,[2] have shown that an automatic mutual recognition in a not fully harmonised area is not possible (as confirmed by the Court of Justice (CJEU)). Therefore, mutual recognition in criminal matters is not an absolute principle.[3] Even though the European Court of Human Rights (ECtHR) Bosphorus decision[4] has referred to an equal level of fundamental rights protection in the EU (in comparison to the ECHR system), Member States, when fulfilling or tolerating mutual assistance/mutual recognition on their territory, are still under the duty to

[1] In the Council general approach text (doc. 14351/1/18, 30 November 2018) even this limited test has been almost entirely abandoned and only a notification for content data, without a possibility of a real reaction, introduced (see Articles 5 and 7a of the Council text).
[2] See FD 2002/584/JHA
[3] See CJEU, Aranyosi and Căldăraru**,** Joined Cases C-404/15 and C-659/15 PPU, and Judgment in Case C-216/18 PPU, *Minister for Justice and Equality v LM*. This was also clearly stated by the ECtHR in its *Avotinš v. Latvia* judgment (ECtHR, a. no. 17502/07, judgment of 23 May 2016) referring to mutual recognition in civil law. This even more applies in criminal law.
[4] ECtHR, *Bosphorus v. Ireland*, a. no. 45036/98, judgment of 30 June 2005.

fulfil the ECHR obligations. In that regard, a strong indication has been provided, that the Commission proposal could raise questions in view of the ECHR case law on Article 8.[1] Furthermore, any broadening of the interpretation of the Treaties, as potentially applied for the legal basis of the proposal regarding the criminal law prerogatives given to the Union, risks to trigger a dangerous rekindling of the 'Solange' debate about the primacy of EU law by national constitutional courts.[2]

Electronic data

With more and more technologies being used e-evidence is likely to become the most important form of evidence in future criminal proceedings. E-evidence is the denomination for several types of data, such as subscriber data, traffic and location data, and content data. The Commission, in its proposal, has introduced four categories, namely: (a) subscriber data, (b) access data, (c) transactional data and (d) content data.[3] Depending on the categories, a request would have to be validated, by either a prosecutor or a judge. Regarding transactional and content data, only a judge could validate an order. The sensitivity of the various types of data, in particular the so-called meta data, has been highlighted by the CJEU ("means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives")[4], as well as several national constitutional courts regarding data retention.[5] Consequently, the proposal touches up extremely sensitive data that can provide a full picture of a person's life, opinions and habits. Yet, the definitions in the proposed Regulation regarding the data categories partly overlap, for example, regarding dynamic IP addresses, so that sensitive meta data might fall under the new category of transactional, but also under the allegedly less intrusive category of "access data" for which lower threshold would apply.[6] Furthermore, issues arise also with the mismatch of these categorisations of data with the definitions of data categories as established in other instruments of EU law in the area of data protection and privacy of electronic communications. Moreover, one must keep in mind that different national and constitutional rules exist regarding the access to such data and in some Member States there is the need for a court authorisation regardless of the categories of data.[7]
Having said that, it is clear that any lowering of data protection or privacy standards has to be avoided. In addition, no difference between the rights and safeguards provided to concerned persons in the real and the virtual world should be made or be considered acceptable.

[1] See, for example, ECtHR case law *Benedik v. Slovenia*,. a. no. 62357/14, judgment of 24 April 2018, *Bărbulescu v. Romania*, a. no. 61496/08, judgment of 5 September 2017, *Roman Zakharov v. Russia* a. no. 47143/06, judgment of 4 December 2015, *Rotaru v. Romania*, a. no. 28341/95, judgment of 4 May 2000, etc. See also ECHR Judge Prof. Bošnjak's presentation in the EP hearing on e-evidence on 27 February 2018.
[2] See the Bundesverfassungsgericht BVerfG, 2 BvE 2/08 referring to strict interpretation of criminal law provisions of the Treaties. The principle of primacy of EU law is not mentioned directly in the Treaties but only in a declaration to the Treaties referring to ECJ case law. In the last years several national constitutional courts re-started the "solange" issue as regards new EU prerogatives in criminal law (for example, CJEU, *Melloni*, , C-399/11, or *M.A.S. and M.B*, C-42/17 - "Taricco 2"). Therefore, a cautious, legalistic and evolutionary approach is necessary in the field of EU criminal law not to damage the basis structure of the Union
[3] Article 2 of the proposal.
[4] CJEU, *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12, and *Tele2 Sverige*, Joined Cases C-203/15 and C-698/15.
[5] BVerfG, Judgment of the First Senate of 2 March 2010 - 1 BvR 256/08 - paras. (1-345). See, *inter alia*, also the decisions of the Austrian, Czech, Romanian and Slovenian constitutional courts.
[6] See, for example, the critical assessment of the EDPB (European Data Protection Board), the CCBE, etc.
[7] See ECtHR, *Benedik v. Slovenia*, see above. See also EJN (the so-called comparison under "fiches belges" - https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelges.aspx).

Fundamental rights, dual criminality and procedural rights

The Commission proposal proposes to transfer certain rights and obligations to private telecommunication and service providers, asking them to check the authenticity of the orders, as well as the legality and the validity of the order (including an assessment of fundamental rights)[1], based on narrow information provided for in the certificate accompanying the order. This is a task that so far, has only been entrusted to national authorities. It is doubtful whether private companies should have the authority or ability to perform such a task. Only in case of non-compliance of the service provider, the enforcement authority of the second state would be involved, yet, without a real possibility to reject the order. On the contrast, regarding cases of conflict with a third country law, a special court litigation process is foreseen in the proposal. Nevertheless, it would be up to a competent court in the issuing country to review the order and if it decides to uphold the order and has not received an objection from the third country, the order would automatically be upheld.[2]
Further doubts persist regarding the scope of the Regulation and the criminal offences for which a production and a preservation order could be issued. According to the proposal, preservation orders, as well as production orders for subscriber and access data, could be issued for all criminal offences; production orders for transactional and content data for all criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years. With this, the principle of dual criminality will no longer apply, meaning that orders could be sent for offences that are not deemed criminal in the Member States where the service provider is located. Bearing in mind the limited amount of harmonisation in criminal law between Member States regarding, on the one hand, the definition of crimes (e.g. definitions of rebellion against the state[3], limits to freedom of expression, abortion rights, etc.), as well as the respective national rules regarding investigations of these crimes, the proposal goes much further than the current mutual recognition system in EU criminal law.
The problem is further aggravated by the fact that the proposal only poorly addresses procedural rights guarantees. Despite the obligation of issuing authorities to provide notice about criminal investigation/right to information, the proposal allows for the issuing authority to request the service provider to refrain from informing the person whose data is being sought and can request to delay the information “as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings”. Apart from that, the proposal only allows for a right to an effective remedy to be exercised before a court in the issuing state in accordance with its national law, even if the affected person might not reside in this country, let alone is able to speak the language or know the legal system of that Member State.

Conclusion

Above, the Rapporteur has presented some of the serious legal questions that need to be addressed in a comprehensive manner.
With regards to the numerous consultations conducted so far (in shadows’ meetings, the LIBE hearing, as well as in bilateral meetings with involved parties), but also publications received (in particular "An assessment of the Commission’s proposals on electronic evidence",

[1] See Article 14 of the initial proposal (“based on the sole information contained in the EPOC, it is apparent that it manifestly violates the Charter or that it is manifestly abusive”). However, in the Council last text (general approach) even this limited test (by a private provider) has been deleted by the majority of Member States.
[2] See Articles 15 and 16 of the Commission proposal.
[3] See the decision of German courts as regards the EAW in the Puigdemont case.

commissioned by the EP Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee),the Rapporteur together with the shadows has identified several legal areas that will need further clarification, in order to guarantee the drafting of a legally sound legal instrument regarding the production and preservation of e-evidence. Consequently, further topical working documents, drafted in the co-rapporteurship, between the Rapporteur and the shadows, will provide for a more detailed analysis. The topical working documents to be drafted are the following:

- Scope of application and relation with other instruments
- Execution of EPOC(-PR)s and the role of service providers
- Relation with third country law
- Conditions for issuing an EPOC(-PR)
- Safeguards and remedies (including data protection safeguards)
- Enforcement of EPOC(-PR)