



All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order

Stanislaw Tosza 

Utrecht University, the Netherlands

Abstract

The European Investigation Order (EIO) was supposed to offer a comprehensive solution to cross-border gathering of evidence within the area of freedom, security and justice replacing a patchwork of instruments and providing for one single standardised order for all types of evidence. However, not even a year since the deadline for its implementation had passed, the Commission proposed an instrument that would be applicable for electronic evidence: European Production Order (EPO). This initiative was born from an increasing frustration in gathering this type of evidence and the conviction that the EIO is not suitable for that purpose. The need for digital evidence (according to the estimate of the EU Commission, 85% of criminal investigations require electronic evidence) is a direct consequence of the place information and communication technology has taken in everyday life. However, electronic evidence differs in a number of ways from ‘real-life’ evidence rendering current legal framework extremely impractical for law enforcement. One of the major obstacles that law enforcement authorities encounter is the fact that the data they need are often stored abroad or by a foreign service provider. Both instruments were conceived because of the need to gather evidence across borders; however, the transnational component is different (evidence being abroad vs. service provider being foreign). Both instruments subject ‘European citizens to the investigative machinery of any other Member State’, however, in a different way. If the e-evidence package is adopted, it will create a dual system of cross-border gathering of evidence, with different philosophy, procedure, enforcement and protective framework. The goal of this article is to analyse and compare two different models of

Corresponding author:

Stanislaw Tosza, Utrecht University, Willem Pompe Institute, Newtonlaan 201, Utrecht 3584 BH, the Netherlands.

E-mail: s.tosza@uu.nl

acquiring evidence that these two instruments offer as well as to delimitate their (non-exclusive) scope. The concluding part will provide a reflection on the systemic consequences of this duality of instruments and of introducing the EPO model in particular.

Keywords

Evidence, criminal investigation, electronic evidence, European Investigation Order, European Production Order, cross-border evidence gathering, European Criminal Law

Introduction

With the right to liberty as the paramount human freedom, the application of the mutual recognition principle to requesting persons for criminal proceedings or execution of sentence was conceived relatively early and the framework decision (FD) on European Arrest Warrant has been functioning for almost two decades already. Applying it to cross-border gathering of evidence has been a much tougher nut to crack.¹ The European Evidence Warrant (EEW) was adopted only in 2008 and its scope was limited. Eventually the European Investigation Order Directive (EIOD) was adopted in 2014 and it was supposed to offer a comprehensive solution. But already before it entered into force, the Commission opened the discussion on a potential instrument that would offer an alternative legal framework for electronic evidence.

This debate resulted in the proposal of the Commission issued in April 2018 of a package consisting of a regulation and a directive aiming at creating a legal framework allowing law enforcement in one member state to directly request service providers in another member state to produce or preserve data (European Production Order – EPO).² While the regulation is the main instrument of the package, the directive should ensure that service providers in the EU designate representatives entitled to receive and comply with the orders. The Council issued a general approach in December 2018³ and it is now for the EU Parliament to formulate its position.

Both instruments were conceived because of the need to gather evidence across borders; however, the transnational component is different (evidence being abroad vs. service provider being foreign). Both instruments subject ‘European citizens to the investigative machinery of any other Member State’,⁴ however, as it will be shown below, in a very different way. If the e-evidence package is adopted, it will create a dual system of cross-border gathering of evidence, with a different philosophy, procedure, enforcement and protective framework.⁵

-
1. John R Spencer, ‘The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: The Reaction of one British Lawyer’ (2010) *Zeitschrift für Internationale Rechtsdogmatik*, 602, 603 ff.
 2. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters [2018] 2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [2018] COM/2018/226 final.
 3. Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – general approach [2018] 15292/18.
 4. Ines Armada, ‘The European Investigation Order and the Lack of European Standards for Gathering Evidence’ (2015) 6 NJECL 8, 9.
 5. Some previous instruments remain applicable, see below.

The goal of this article is to analyse and compare the two different models of acquiring evidence that these two instruments offer as well as to delimitate their (non-exclusive) scope. The concluding part will provide a reflection on the systemic consequences of this duality of instruments and of introducing the EPO model in particular.⁶

European Investigation Order

The European Investigation Order (EIO) was not the first attempt to address the problem of cross-border evidence gathering at EU level. The European Convention on mutual assistance in criminal matters of 29 May 2000 provided a framework based on the traditional MLA approach. To this, two mutual recognition instruments were added: first, the FD on freezing orders was adopted in 2003,⁷ and then the FD on the EEW in 2008.⁸ Since the entry into force of the latter, the legal instruments of cross-border preservation and exchange of evidence were meant to be: freezing orders and EEW for existing evidence and MLA letters rogatory for the investigative measures not concerning the latter.⁹

This combination of instruments was necessarily complicated and hence impractical. More importantly, some member states did not even proceed with the implementation of the EEW FD.¹⁰ Already a year after the adoption of the EEW FD, the Stockholm programme declared that a new comprehensive solution had to be found.¹¹ While the Commission proposed in a Green Paper a new approach including admissibility of evidence,¹² some member states went around it by proposing the EIOD. The latter was silent on the issue of admissibility. The latter approach won and the EIOD was adopted on 3 April 2014.

The Directive replaces the patchwork of instruments providing for one single standardised order for all types of evidence, with two exceptions: setting up of or gathering evidence within joint investigation teams,¹³ and cross-border surveillance provided for in the Convention implementing

6. The e-evidence initiative is subject to intense debate as to a variety of its aspects. Among the problems discussed is the question of the legal basis and whether the EPO is in fact a mutual recognition instrument. This complex issue merits a separate publication, hence it will not be discussed in this article.

7. Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, OJ L196/45.

8. Framework Decision on the European evidence warrant.

9. Marcello Daniele, 'Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles' (2015) 6 NJECL 180. To complete this picture, one should add 'spontaneous transmission' of information between prosecutorial authorities that cannot become evidence at trial but can be used to decide on investigative measures such as arrest or search (Silvia Allegrezza, 'Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality' in Stefano Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014) 57). See on that Michele Simonato, 'Spontaneous exchange of information between European judicial authorities from the Italian perspective' (2011) 2 NJECL, 222–229.

10. For example, Austria, Italy or Sweden. Austria and Sweden will be among the seven member states that proposed the EIO Directive. <https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?l=EN&CategoryId=40>

11. Council of the European Union, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, [2009] 17024/09, 22.

12. Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility [2009] COM/2009/0624.

13. The instrument for that is EU MLA Convention Art. 13 and the Council Framework Decision of 13 June 2002 on joint investigation teams. EIO would still apply to situations where evidence is being sought from a Member State other than one of those that have set up the JIT (Art. 3 EIOD, last part of the sentence).

the Schengen Agreement.¹⁴ The EIO is based on mutual recognition with orders circulating between and executed by competent authorities with a number of non-mandatory grounds for refusal. The EIOD also replaces the Directive on freezing, but only as regards freezing of evidence, but not regarding confiscation, which is being dealt with by another – also comprehensive – instrument.¹⁵

The Directive was adopted after a significant debate centred mainly around fundamental rights issues and admissibility of evidence.¹⁶ While the instrument provides for a unified framework, it does not attempt to unify or harmonise the law of evidence, leaving fully in the hands of the member states decisions on the conditions for issuance, competent authorities for particular types of measures and remedies. Despite not being so revolutionary, the implementation period was fairly long – more than 3 years.¹⁷

An EIO is a judicial decision to have specific investigative measure(s) carried out in another MS with the objective to obtain evidence.¹⁸ Thus, and contrary to the EEW, the focus of the decision is the measure and not particular pieces of evidence, the obtaining of the latter being the purpose of the measure. This of course does not preclude the measure from relating to evidence that is already in the possession of the competent authorities. The EIO may be issued for any kind of investigative measure, with the two exceptions mentioned above.

In addition to the general framework, some measures are singled out, such as hearing by video- or telephone conference, gathering information on bank and other financial accounts or operations, controlled deliveries or covert investigations. No special rules are foreseen for production orders, but these are clearly included. However, a special chapter on interception of telecommunications provides a few additional rules regarding these measures (Arts 30 and 31 EIOD).

14. Article 3 and Recital 9 EIOD.

15. Article 34 (2) EIOD; Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders; José Eduardo Guerra, Christine Janssens, Legal and Practical Challenges in the Application of the European Investigation Order, [2019] *eucrium* 46, 48.

16. It is impossible to list the whole publication list on this issue here. Interested readers may consult for instance the following publications: Silvia Allegrezza, 'Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from One Member State to Another and Securing its Admissibility' (2010) *Zeitschrift für Internationale Rechtsdogmatik* 569 ff.; Lorena Bachmaier Winter, 'European Investigation Order for Obtaining Evidence in the Criminal Proceedings. Study of the Proposal for a European Directive' (2010) *Zeitschrift für Internationale Rechtsdogmatik* 580 ff.; John R Spencer, 'The Green Paper on Obtaining Evidence from one Member State to Another and Securing its Admissibility: the Reaction of one British Lawyer' (2010) *Zeitschrift für Internationale Rechtsdogmatik* 602 ff.; Gert Vermeulen, *Free Gathering and Movement of Evidence in Criminal Matters in the EU: Thinking Beyond Borders, Striving for Balance, in Search of Coherence*, (Maklu 2011). For further critical analysis, see for instance, Silvia Allegrezza, 'Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality' in S. Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014); Lorena Bachmaier Winter, 'The Proposal for a Directive on the European Investigation Order and the Grounds for Refusal: A Critical Assessment' in Stefano Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014); John Vervaele, 'Reconocimiento Mutuo y Prueba Administrativa y Penal Europea en el Espacio Europeo de Justicia Penal' in M^a Isabel González Cano (ed), *Orden Europea de Investigación y Prueba Transfronteriza en la Unión Europea* (Tirant lo Blanch 2019) and other contributions to these books.

17. For example, the implementation period for the European Arrest Warrant FD was approximately 1.5 years, for the EEW FD, it was approximately 2 years.

18. Article 1 EIOD.

An EIO may be issued in criminal proceedings (Art. 4 (a) EIOD), but not only. Three other contexts are foreseen:

(b) in proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters;

(c) in proceedings brought by judicial authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters; and

(d) in connection with proceedings referred to in points (a), (b) and (c) which relate to offences or infringements for which a legal person may be held liable or punished in the issuing State.¹⁹

However, for points (b) and (c), the executing state may refuse execution if the measure would not be authorised under its law in a similar domestic case.²⁰

It is for national law to decide which authority is competent for which measure (Art. 6 (1)). The EIOD contains two catalogues of competent issuing authorities. The first is closed and contains judges, courts, investigating judges and public prosecutors. These authorities may issue an EIO if the national law entitles them to that. The second catalogue is open and contains

any other competent authority as defined by the issuing state which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law.”

However, the EIO issued by these authorities must be validated by the authorities from the first catalogue regarding the fulfilment of conditions of issuance.²¹ While this validation procedure (general judicial reservation, *Justizvorbehalt*²²) should prevent the use of EIO without judicial control of investigative measures, it still triggers fear of overuse by the Police, if the judicial validation becomes mere rubberstamping.²³ In addition to that, if national defence rights so permit, the issuing of an EIO may be requested by an accused person or a suspect.²⁴

The conditions of issuing an EIO are in the first place necessity and proportionality (to the purposes of the proceedings in question). The measure must be available in the issuing state and ordered under the same conditions as would be necessary to its issuance in a similar domestic case.²⁵ While leaving it to the member states to legislate on these conditions, it also becomes a barrier against forum shopping.²⁶ Double criminality is not a condition as such; it is only an

19. Article 4 EIOD.

20. Article 11 (1) d EIOD.

21. Article 2 EIOD.

22. Kai Ambos, *European Criminal Law* (Cambridge University Press, Cambridge 2018) 456.

23. Ines Armada, ‘The European Investigation Order and the Lack of European Standards for Gathering Evidence’, (2015) 6 NJECL 11–12. Anne Weyembergh, ‘Transverse Report on Judicial Control in Cooperation in Criminal Matters: The Evolution from Traditional Judicial Cooperation to Mutual Recognition’ in: Katalin Ligeti (ed), *Toward a Prosecutor for the European Union*, Volume 1 (Hart Publishing 2013) 963.

24. Article 1 (3) EIOD.

25. Article 6 (1) EIOD.

26. Ambos, (n 22) 458. On differences between approaches and standards of member states, see Ligeti, (n 23).

optional ground for refusal. In the context of interception of telecommunications, Art. 30 (4) requires the issuing authority to indicate ‘the reasons why it considers the indicated investigative measure relevant for the purpose of the criminal proceedings concerned’, which is normally not necessary.

Unless the executing authority decides to invoke one of the grounds for refusal, it shall recognise the EIO and execute it ‘in the same way and under the same modalities’ as if it concerned a national measure. It shall ‘comply with the formalities and procedures expressly indicated by the issuing authority’ unless they are contrary to the fundamental principles of law of that member state.²⁷ In principle then, it is the law of the issuing member state that governs the measure, which should ensure its later admissibility.²⁸

The order should be treated and executed with the same celerity and priority as in a similar domestic case and if possible take into account requests of the issuing authority in that respect. Two concrete deadlines are foreseen for the order: for the decision on the recognition or execution no later than 30 days after the receipt and for the execution 90 days following the taking of the decision.²⁹ These deadlines are not absolute. The deadline for execution or recognition may be extended by 30 days; as to the delay for the execution (or the specific requests of the issuing authority in that respect), if it is not possible to comply with these deadlines, the executing authority shall consult with the issuing authority to find appropriate timing.³⁰ It is also possible to postpone the recognition or execution of the EIO because of the interests of an ongoing criminal investigation or prosecution.³¹ It is for the executing state to decide what is the reasonable delay in that case.

The EIO offers the executing authorities a number of grounds for refusal, which can be summarised into the following points:

- immunity or privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media;
- issues of national security interests, protection of the source of information or secrets of intelligence activities;
- ne bis in idem;
- territoriality (offence committed outside the territory of the issuing State and wholly or partially on the territory of the executing State)
- fundamental rights issues
- lack of double criminality (limited to certain offences)
- measure not available under the law of the executing state for this offence, because its use is restricted to certain offences.³²

27. Article 9 (1) and (2) EIOD.

28. Daniele, (n 9) 179, 182. See also André Klip, *European Criminal Law. An Integrative Approach* (3rd edn, Intersentia 2016) 394ff, 400 ff.

29. Article 12 EIOD.

30. Articles 11 (5) and (6) EIOD.

31. Article 15 EIOD.

32. Article 11 (1) EIOD.

Besides the last ground, the executing state may not, in principle, refuse the order because it would not have been authorised in a similar domestic case. However, this ground is available exceptionally for interception of communications.³³

Before invoking one of the refusal grounds (except the ones regarding the types of proceedings or double criminality), the EIOD obliges the executing authority to enter into dialogue with the issuing authority including potentially requesting additional information.³⁴

Instead of executing the requested measure, the executing authority may undertake a different investigative measure in two situations. Firstly, if this other measure is less intrusive, but may achieve the same result. Secondly, if the requested measure is not available at all or would not be available in a similar domestic case. Some enumerated investigative measures always have to be available under the law of the executing state, for instance: ‘the identification of persons holding a subscription of a specified phone number or IP address’.³⁵ Despite the overall mutual recognition philosophy, the possibility to make the assessment whether a less intrusive measure could be used creates a possibility for a verification of the order’s proportionality and necessity by the executing authority.

Besides these obligations, the EIOD does not provide – unsurprisingly – any way of forcing the executing state refusing to execute the EIO to do so. The only potential reaction is triggering the procedure for non-implementation of a directive, which will be of little use for a concrete request.³⁶

The EIOD does not provide for concrete remedies but stipulates that ‘legal remedies equivalent to those available in a similar domestic case’ must be applicable. It limits the possibility to question the ‘substantive reasons’ for issuing the EIO to actions brought in the issuing state.³⁷

The EIO may also be issued for freezing evidence. The Directive contains one provision in that respect regarding the deadlines and questions of whether the items in question should be kept. As to the time limits, the EIOD backtracks on the celerity of the procedure offered by the FD on freezing orders which required in principle immediate execution,³⁸ and the competent authorities were supposed to ‘decide and communicate the decision on a freezing order as soon as possible and, whenever practicable, within 24 hours of receipt of the freezing order’.³⁹ The same deadline is kept as to the latter aspect, but no deadline for execution is given. Hence the general rule for all the EIO applies: the authorities should act with the same celerity and priority as for a similar domestic order and comply with the 90-day extendable deadline.

European Production and Preservation Orders

Background and e-evidence proposal

The European Production and Preservation Orders (they will be called EPO when analysed together and if only one of them is meant: EPdO and EPsO, respectively)⁴⁰ have been conceived

33. Article 30 (5) EIOD.

34. Article 11 (4) EIOD.

35. Article 10 (2) EIOD.

36. Articles 258 and 259 TFEU.

37. Article 14 EIOD.

38. Article 5 (1) Freezing Orders FD.

39. Article 5 (3) Freezing Orders FD.

40. This article suggests a change in the abbreviations used for these instruments. The abbreviations proposed by the Regulation are rather unfortunate. EPOC for the production order and EPOC-PR for the preservation order. Since both words – production and preservation – start with the letters ‘PR’ the risk of confusion is high. In view of the author, the

out of a similar need to gather evidence cross-border and frustration that the current framework is not sufficiently workable. Nonetheless, the reasons for this frustration had a different source, linked with technological developments that clashed with traditional legal concepts such as territoriality and jurisdiction, and the need to have access to digital evidence which has been growing exponentially.⁴¹

This need is a direct consequence of the place information and communication technology has taken in everyday life. It is a truism to say that with everyday human life having increasingly digital existence, the need for electronic evidence is increasing with the same pace. However, electronic evidence differs in a number of ways from ‘real-life’ evidence rendering the current legal framework extremely impractical for law enforcement.

First of all, digital evidence is held on servers owned by service providers. Service providers are often foreign, and given the dominance of the market by major service providers (Google, owning also YouTube; Facebook, owning also Instagram and WhatsApp; Microsoft owning also Skype; Apple and Amazon) most often American. Data may be managed by subsidiaries of these companies headquartered in Europe. The picture is even more complicated as servers may be stored in data centres potentially located in yet another country. For instance, Facebook’s enormous data centre is located in Luleå, Sweden.⁴² Yet, investigation and prosecution is confined to national borders and if it goes beyond it, instruments of international cooperation must be used. These are time-consuming and cumbersome.⁴³

Secondly, the territorial approach to the jurisdiction to enforce – that is, based on the location of data – is not only impractical, but also in the process of becoming technologically outdated, given the growth in use of cloud computing.⁴⁴ Furthermore, data might be transferred in a way where data are not stored on a single server, hence subsequent requests cannot be fulfilled.⁴⁵ Lastly, the investigation authorities depend much more significantly on cooperation of service providers also for practical reasons. While a raid on a company that refuses to produce requested documents would be a viable possibility, a raid on a data centre would not bring similar (if any) results, unless

abbreviation EPdO and EPsO would be much easier for an immediate recognition of which instrument is being referred to, and also in the spoken language. It would also be much easier for the respective certificates: EPdOC and EPsOC.

41. ‘Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction’. – Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, 1.
42. <<https://www.datacenterknowledge.com/facebook/facebook-data-center-investment-sweden-nears-us1b>>
43. Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2 December 2016, 15072/16, p 5.
44. Jennifer Daskal, ‘The Un-Territoriality of Data’ (2015) 125 YLJ 326–398. Vivek Krishnamurthy, ‘Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters’, Berkman Klein Center Research Publication No. 2016-3 (18 February 2016), <<https://ssrn.com/abstract=2733350>>.
45. For example, P2P technology of Skype, Vanessa Franssen, ‘The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?’ (2017) 3 Eur. Data Prot. L. Rev., 534, 538; Salman A Baset and Henning G Schulzrinne, ‘An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol’, <http://www1.cs.columbia.edu/~salman/publications/skype1_4.pdf>. Nota bene, Skype recently changed its technology. <<https://www.lifewire.com/skype-changes-from-p2p-3426522>>

disproportionally significant forces are used to find the necessary data, potentially including heavy decrypting capacities, if that was possible at all.⁴⁶

To overcome these problems, law enforcement has tended to resort to voluntary cooperation or abandoning the territorial approach. The former, consisting in sending requests to service providers to which they are not obliged to respond, lacks an enforcement mechanism and framework of protection of rights for persons affected. The example of the abandoning of territoriality was delivered by Belgium, first in case law and then in its code of criminal procedure, through which it extended obligations of cooperation to service providers offering services targeting Belgian citizens, regardless of the location of data or the service's headquarters.⁴⁷ Yet, this approach puts a strain on the service providers as they may find themselves in a conflict of legal obligations, if the legal framework related to their headquarters or location of data forbids them to provide thus requested data.⁴⁸

The increasing need to obtain data for criminal investigation combined with these difficulties and the volatility of data creates the need to find a solution which would facilitate this process. The EIO may serve to acquire electronic evidence, but it is claimed that for that its deadlines are too long and create risk that data disappears or is altered in the meantime.⁴⁹ Nor can it resolve the question of territoriality.⁵⁰ Hence, even before the EIO date of implementation passed, the EU Commission was requested by the Council to begin a reflection on a solution to these problems.⁵¹ This resulted in two non-papers⁵² and further documents, including a thorough impact assessment.⁵³ The key question of the debate was whether to introduce an instrument which would be limited to allowing service providers to provide data requested by the authorities of a member state

46. On technical and legal issues related to this problem, see: Katalin Ligeti, Gavin Robinson, 'Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?' in Robert Kert, Andrea Lehner (eds), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag* (NWV 2018) 625–644.

47. Franssen, (n 45).

48. That was the case in both cases: Yahoo: US law; Skype: Luxembourgish law.

49. Commission Staff Working Document, Impact Assessment, Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Brussels, 17 April 2018 SWD (2018) 118 final) 23.

50. The system offered by the EPOR and the Directive breaks with the logic of territoriality (in the sense of linking jurisdiction to enforce with the location of data). The EIOD does not provide any provisions in that respect and hence rest within the latter logic (stemming from the famous judgment of the Permanent Court of International Justice on 7 September 1927 in the case of *SS Lotus*, Publications of the Permanent Court of International Justice, Series A.-No. 70, 18–19). On the problem of jurisdiction, see inter alia: Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017).

51. Conclusions of the Council of the European Union on improving criminal justice in cyberspace [2016] ST9579/16.

52. Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2 December 2016, 15072/16; Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 22 May 2017, <https://ec.europa.eu/home-affairs/sites/home-affairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf>.

53. Commission Staff Working Document, Impact Assessment, Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Brussels, 17 April 2018 SWD (2018) 118 final).

different than the one where they are established, but without compelling them to do so (it would already tear down barriers of national legislation forbidding it), or whether the orders would be mandatory.⁵⁴

The latter approach won. The Commission's proposal introduces a mandatory order which – if the proposal is adopted – competent authorities in one member state address to service providers in another one, in principle without engaging authorities in that member state. Furthermore, it abandons territoriality as the principle deciding where orders are to be addressed. According to this new system, the service providers would be obliged to designate at least one legal representative in the EU for the 'receipt of, compliance with and enforcement of' these orders.⁵⁵ Failure to do so would mean that the authorities may send the order to any establishment of the service provider in the EU.⁵⁶ These duties affect all service providers 'offering services in the Union'.⁵⁷ This concept does not mean that every service accessible from the EU falls into the scope of the directive and regulation, but it is fairly broad. In particular, the location of data is without importance for deciding whether the request may be issued and to which place it should be addressed.

This approach may put service providers in conflict with legislation outside of the EU, in particular the American one, as explained below. The conflict may be even graver – potentially – as the regulation permits to request for data of non-EU citizens. The regulation addresses the question of conflict of legal obligations. The practical success of EPO depends also on whether it is done in a satisfactory way, as numerous legal conflicts of significant providers may jeopardise the use of the orders.

In that respect, it is important to note the negotiations that the EU is conducting with the US for an agreement under the recently enacted CLOUD (Clarifying Lawful Overseas Use of Data) Act. In principle, US legislation (Electronic Communications and Privacy Act 1986) forbids its service providers to share content data with foreign law enforcement outside of the MLA procedure (non-content data may be shared voluntarily).⁵⁸ The CLOUD Act would lift this so-called blocking provision provided that the United States signs an agreement with the country in question based on the assessment of that country's rule of law and privacy protection.⁵⁹ For the consistency of the area of freedom, security and justice (AFSJ), it is of paramount importance to have one EU-US agreement in that respect instead of a fragmented patchwork of different agreements and member states not (yet) having it. By introducing one instrument of cross-border exchange of electronic evidence at the EU level, the EU should become a preferred partner of the United States.⁶⁰

The Regulation (EPOR) contains also the possibility to preserve data in view of subsequent request for production of thus preserved data not only via an EPdO but also mutual legal assistance or an EIO.⁶¹

54. Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 22 May 2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf>, 4–5.

55. Article 3 (1) of the Directive.

56. Article 7 (2) of the Regulation (EPOR).

57. Article 2 (1), (2), (4) EPOR.

58. Jennifer Daskal, 'Unpacking the CLOUD Act', [2018] 4 *eucrim*, 220–225, 222

59. *Ibid.*, 220 ff.

60. Recommendation of 5 February 2019 for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM (2019) 70 final. The Council took the positive decision on 21 May 2019, Doc. 9114/19

61. Article 6 (2) EPOR.

At this point, there exist two versions of the text: the original Commission proposal and the Council's general approach. While the latter version aims at solving a number of problems, the fundamental elements of the order's design remain the same. The article will signal instances where the two versions differ. It is important to note already at this point that the draft regulation contains an express provision that it does not preclude the use of EIO.⁶²

European Production Order

“European Production Order” means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence’.⁶³

The term electronic evidence is also defined by the EPOR, but in a less direct way. It should be understood as evidence stored in electronic form by or on behalf of a service provider at the moment of reception of the order and consisting of one of the four categories of data: subscriber, access, transactional and content data. Each of these categories is defined in Art. 2 EPOR as well. It seems an unfortunate legislative technique to define electronic evidence with the requirement of having it available by the service providers at the time of order's receipt. It is more a question of application of the instrument than a question of what is or is not digital evidence. This aspect will be relevant for delineating the scope of EPO and EIO.

The answer to the question of who may issue an EPdO depends on the type of data being sought. Judges, courts or investigating judges may issue orders for any type of data. The prosecutors' competence in that respect is limited to subscriber or access data, as these categories are perceived as less intrusive and hence do not require the same level of ex ante scrutiny.⁶⁴ Furthermore, and similarly to EIO, ‘any other competent authority [...] acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law’ may also issue an EPO, but the latter must be validated by an authority entitled to issue it in its own right.⁶⁵

The EPO may be issued only for criminal proceedings and – in the version of the Council – also for the execution of custodial sentences.⁶⁶ In that sense, the EPO has a narrower (than EIO) scope of application. The General Approach adds also that the Regulation should not apply if the purpose of gathering digital evidence would be to provide mutual legal assistance to another member state or a third country.⁶⁷ The orders may also be issued in proceedings against legal persons, similarly to the EIO.⁶⁸

62. Article 23 EPOR.

63. Article 2 (1) EPOR.

64. EPOR Explanatory Memorandum, 14-15.

65. Article 4 (1) – (3) EPOR.

66. Article 3. (2) EPOR (General Approach version): the exact expression reads: ‘for the execution of custodial sentences or detention orders that were not rendered in absentia in case the convict absconded from justice’. This formulation is unfortunate, as it seems only to exclude in absentia proceedings where the reason for this exclusion was the fact that the convict absconded from justice and making it possible to issue EPO for persons convicted in absentia for any other reason. The reason for differentiating these two reasons for in absentia proceedings is not visible and it seems at odds with the explanation of this point added to the Explanatory Memorandum by the Council in Recital 24b.

67. Article 3 (1a).

68. Article 3 (2) last sentence.

While the recipient of an EIO is a competent authority, the recipient of the EPO is a service provider offering services in the Union and established or represented in another member state and the EPO is limited to data pertaining to services as described below.⁶⁹ It is worth paying closer attention to the definition of service provider as the data may only be sought through EPO if there is a provider to which it may be addressed. If there is none, EIO remains the only option.

A service provider can be a natural or a legal person and is otherwise defined by services it offers which can be:

- electronic communication services,
- information society services,
- Internet domain name and IP numbering services.⁷⁰

The details of definitions of both categories are divergent between the original version and the general approach. In practice, the first two categories comprise such services as Skype, WhatsApp, Amazon, Dropbox and mailing services.⁷¹ As to the last category, it makes reference to the providers of Internet infrastructure services who hold data that may be of high relevance for identifying persons of interest.⁷² The General Approach excludes financial services referred to in Art. 2(2)(b) of Directive 2006/123/EC.

Providers of services described above fall into the scope of the draft regulation only if they are offering services in the Union and are established or represented in another member state. From the perspective of legislative technique, this is a cumbersome way of explaining relatively basic premises of the regulation.⁷³ The regulation defines what it means to offer services in the Union: it means to enable legal or natural persons in at least one member state to use services described above and having a substantial connection to that or these member state(s) (Art. 2 (4)). So the regulation does not only apply to the service providers established in the Union, but it is enough that they offer services in the Union. It follows the philosophy that profiting from these services in the Union creates also obligations towards law enforcement in the same geographical area and also creates a level playing field between the providers in terms of obligations and avoiding an easy to use gap in law enforcement.⁷⁴

However mere accessibility of the service from the Union cannot be a sufficient criterion, as this would make every provider in the world fall into the scope of the provisions of this regulation. In the simplest situation, the substantial connection element results from the fact that the service provider has an establishment in at least one member state. In the absence of that connection, it can be established ‘on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member

69. Article 3. (1) and Article 2. (1), Article 3. (3) EPOR.

70. Article 2 (3) EPOR.

71. Vanessa Franssen, ‘The European Commission’s E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?’, European Law Blog, published on 12 October 2018, <<https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/>>.

72. Explanatory Memorandum, Art. 2.

73. Also on that point, Art. 3 defines the scope of the regulation, but the definitions of the EPsO and EPdO in Arts (1) and (2), respectively, present better the scope, as the regulation does not apply to national situations, which is explained in the latter and not mentioned in the former.

74. Explanatory Memorandum, Art. 3.

States'.⁷⁵ As to the latter criterion, the Explanatory Memorandum gives examples of factors determining that the service provider targets its services towards a member state: use of a language or currency of that state, or providing local advertising. While this does not seem problematic, the former criterion may lead to a more troublesome result: if a service becomes very popular with a significant number of EU users, without it being a particular intention of the service provider, it may make it fall into the scope of the regulation.

Furthermore, the service provider has to be established or represented in another member state of the Union, as otherwise it would be a purely domestic situation, which is excluded from the scope of the draft regulation. It stems (only!) from the definitions of the EPdO and EPsO, respectively, that the order cannot be used in a national context. However, what is omitted from the regulation is the question of how to determine when the data are held by or on behalf of a service provider established or represented outside of the issuing member state. That in turn may lead to the use of this instrument to obtain data, when the national criteria are more difficult to meet than those in the regulation.

To issue an EPO, a number of conditions must be fulfilled. The first two resemble the EIO. First of all, 'a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State'. Secondly, the order must be necessary and proportionate for the purpose of the proceedings for which it is being issued.

Thirdly, the issuance of EPO may be limited depending on the offence under investigation. This limitation does not concern orders issued for subscriber or access data. However, an EPdO to produce transactional or content data may only be issued for offences 'punishable in the issuing State by a custodial sentence of a maximum of at least 3 years' or offences enumerated in the acts to which the Regulation makes reference. The latter group is composed of offences harmonised by EU instruments in specific fields such as terrorism, fraud, sexual abuse and sexual exploitation of children and child pornography, attacks against information systems.⁷⁶

The version of the Council adds another condition aimed at solving problems related to the immunities and privileges and to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression. If an order concerns transactional data and there are reasonable grounds to believe that the person whose data are sought is not residing on the territory of the issuing state and the data are protected by the rules of one of the kinds enumerated here, the issuing authority shall first seek clarification on these issues from the competent authorities of a member state concerned. If it results that the order could impact fundamental interests of the other state, these circumstances should be taken into account while issuing the order (including abstaining from its issuance) in the same way as if these rules were part of national law.⁷⁷

Regarding the same problem but for orders concerning content data, the Council added the mandatory notification of a competent authority of the member state concerned. Upon reaction of that authority

the issuing authority shall take these circumstances into account in the same way as if they were provided for under its national law and shall withdraw or adapt the Order where necessary to give effect to these grounds if the data were not provided yet.⁷⁸

75. *Ibid.*

76. Article 5 (4) EPOR.

77. Article 5 (7) EPOR.

78. Article 7a EPOR.

Transmission, reaction, enforcement

The key innovation of the regulation is in its cross-border transmission. Instead of being addressed to the competent authority in another member state, it is addressed directly to the service provider, and more concretely to its legal representative. The EPOR together with the Directive provide for a number of rules aimed at guaranteeing that the transmission reaches the service provider, including sanctions for not designating a representative and the possibility to address the order to any establishment of the service provider.⁷⁹

The order is transmitted to the service provider (i.e. the representative) in form of a certificate (signed and certified).⁸⁰ The certificates are to be transmitted ‘by any means capable of producing a written record allowing the addressee to establish its authenticity’.⁸¹ This expression was tightened by the General Approach of the Council stressing that the certificate has to be transmitted ‘in a secure and reliable way’. This formulation, which may be potentially less stringent than national law of some MSs, opens the possibility of including technical means, that is, platforms or other appropriate digital channels, to fasten and smoothen the transmission of requests. These platforms may be established by service providers; some have already established them.⁸² The platform may also be provided by the public sector: it is under construction by the EU Commission for EIO and MLA requests;⁸³ such a platform exists for exchanging data in cross-border civil procedures (eCodex).⁸⁴

It is important to differentiate between the order and the certificate. The certificate contains standardised – to avoid mistakes – content necessary for the service provider to react to the order. However, the full content of the order, in particular the reasoning regarding necessity and proportionality or other details of the case, is not to be transmitted to avoid negative impact on the case. The latter will be accessible in due course by the suspect and may be subject to applicable challenges.⁸⁵

The default reaction of the ISP should be transmission of the requested data, also directly to the issuing authority (again without any intervention of the authority of the state of the ISP). This should be done within 10 days from the receipt of the order or earlier if requested, and in emergency cases within 6 h.⁸⁶ These are much shorter deadlines than the ones provided by the EIO.

The ISP may find itself in a situation of impossibility to comply with an order. For these cases, the regulation provides for dialogue, aiming at furnishing necessary clarification to the ISP or withdrawing the order. This is in particular the case if the order is incomplete, contains manifest

79. Article 7 EPOR and the Directive. For more detailed analysis see Stanislaw Tosza, The European Commission’s Proposal on Cross-Border Access to E-Evidence Overview and Critical Remarks, (2018) 4 *eu crim*, 212–219, 217 f.

80. The certificates are standardised by the annexes to the Regulation.

81. Article 8 (2) EPOR.

82. EPOR Explanatory Memorandum, 18. For example, Facebook provides a Law Enforcement Online Request System <<https://www.facebook.com/records/login/>>.

83. <https://www.ejn-crimjust.europa.eu/ejnupload/News/Outcome-Report_Eurojust-meeting-on-EIO-Sept-2018_EN.pdf>, 15.

84. Interpol also offers a platform called SIRIUS aimed at sharing ‘knowledge, best practices and expertise in the field of internet-facilitated crime investigations, with a special focus on counter-terrorism’ <<https://www.europol.europa.eu/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations>>. Both SIRIUS and eCodex may be potentially expanded to serve for the purposes of the e-evidence requests: EPOR Explanatory Memorandum, 19.

85. EPOR Explanatory Memorandum, 18.

86. Article 9 (1) EPOR.

errors or does not contain sufficient information to execute it or in cases of de facto impossibility. However, the issuing authority has the upper hand: at no point does the regulation force the issuing authority to withdraw the order.⁸⁷

Non-compliance with the order may trigger two types of consequences: sanctions and enforcement procedure. As to the sanctions, the regulation leaves it to the member states to provide necessary rules in that respect. Interestingly, at no point does the regulation say which state should be responsible for imposing and enforcing it. This would mean that the rules of transnational *ne bis in idem* would apply, leaving uncertainty for the service provider in question. Furthermore, the Council added a clause expecting the member state to ensure the possibility to impose a sanction of up to 2% of the total worldwide annual turnover.⁸⁸ If accepted, such a sanction could theoretically be imposed for one instance of refusal to provide data of one email account in a case of a simple offence that fulfils the threshold of potential 4 years' imprisonment. This may raise eyebrows as it appears not really proportional and in case of big providers would result in extremely huge amounts.

The enforcement procedure turns an EPO into a much more classical mutual recognition instrument and in that sense more similar to EIO. The issuing authority may transfer the order to a competent authority in the enforcing state (*nota bene*, not executing state as in the case of an EIO), who should recognise and enforce the order. Also as in a classical mutual recognition, a number of grounds of refusal may be invoked by the enforcing authority. However, they look very different than the ones in the EIOD or in the EAW FD. They are mainly related to the problems with issuance of the order (the service not covered by the regulation, non-competent authority or offence out of the scope of application of EPOR) or impossibility of executing the order by the provider.⁸⁹ These grounds may be invoked also by the service provider, but the enforcing authority has the last say and may disregard this objection.⁹⁰ The Council added to this list grounds related to the issue of privileges and immunities as well as freedom of press and expression. These may not be invoked by the service provider.

Interestingly, the Council deleted a ground of refusal – already more limited than the EIO equivalent – based on manifest violation of the Charter or of the order being manifestly abusive. It is certain that the Council wanted to make sure that ISPs cannot invoke that reason (which was possible in the previous version). However, lack of this ground may not prevent the enforcing authorities from invoking it. Article 1 (2) EPOR says that '[t]his Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU'. It provides for a similar clause as the one in Art. 1 (3) of the EAW FD, which was the basis for the decision in *Aranyosi/Căldăraru*⁹¹ and more recently in *Minister for Justice and Equality v LM*.⁹²

The list is limited to these grounds. In particular, the list does not include double criminality, *ne bis in idem* or questions of necessity and proportionality. Furthermore, as the instrument is a

87. Article 9 (3) – (6) EPOR.

88. Article 13 EPOR.

89. Article. 4 EPOR.

90. Article 14 (3) and (6) EPOR.

91. Court of Justice of the European Union (CJEU) 5 April 2016, joint cases C-404/15 and C-659/15 PPU, ECLI: EU: C:2016:198.

92. CJEU 25 July 2018, Case C-216/18 PPU *Minister for Justice and Equality v LM*, ECLI: EU: C:2018:586.

regulation, the member state certainly cannot add any further grounds in their national legislation.⁹³

Conflicting obligations and remedies

The EPOR contains a chapter called 'Remedies'. Yet, only a small part of it is devoted to the remedies regarding affected persons and formulates the obligation of the member states to provide for effective remedies for persons whose data were sought.⁹⁴ Most of the chapter, however, contains rules aimed at addressing situations in which compliance with the order would create conflict with law of a third country.

If such conflict exists, the service provider shall inform the issuing authority providing reasons for objecting to the order, in particular all relevant details on the law in question and the nature of the conflicting obligations.⁹⁵ The mere fact that similar provisions regarding production orders do not exist in the third country in question or that the data are stored in a third country is not sufficient to raise this objection. In that sense, the proposal parts with the traditional territoriality principle, which links jurisdiction with the place where the data are stored.⁹⁶ As mentioned already above, this is in line with current trend which for reasons of technological developments (e.g. cloud computing) and impracticality of this solution tend to abandon this approach.

The issuing authority is obliged to review the order in view of the objection and if it intends to uphold it, the order shall be reviewed by a court in the member state of the issuing authority. In principle, even if it comes to the conclusion that a conflict of laws exists, the court is not obliged to withdraw or lift the order, but it has to make an assessment based on a number of criteria, such as a balancing act of fundamental rights and interests, the degree of connection of the case or of the service provider to the third country, the interests of the issuing state and the potential consequences for the service provider of complying with the order.

A very interesting discrepancy exists between the Commission and the Council proposals as regards conflicts of laws where the laws of a third country prohibit disclosure of the data for reasons of necessity to protect the fundamental rights of the individuals concerned or to protect the fundamental interests of that country related to national security or defence. The Council would prefer to treat this category in the same way as any other conflict of laws, thus applying the rules described above. But the original proposal of the Commission offered a different procedure, within which, if the court finds that the conflict with the law of that kind exists, it should address an authority in the third country. If the latter confirms the conflict, the order must be lifted. In case of the authority not reacting even after a reminder within fairly short deadlines provided, the order is upheld, which would put the service provider in an uncomfortable situation as lack of reaction might be caused by bureaucratic slowness and not necessarily shield the provider from sanctions. The proposal of the Council results in that in no scenario EU authorities would be bound to lift the

93. For example, while implementing the EAW FD, some member states added fundamental rights clauses not foreseen in the FD as such, Tony Marguery, *Transfer of Prisoners in the European Union - Towards a better balance between Fundamental Rights and Mutual Trust* (Wolf Legal Publishers 2018) 421.

94. Article 17 EPOR.

95. Article 15/16 (1) and (2) EPOR.

96. As exemplified in the decision of the US Court of Appeals for the Second Circuit, in re Microsoft Corp. (so-called Microsoft Ireland Case), 829 F.3d 197 (2nd Cir. 2016).

order resulting in the conflict of law, potentially increasing the number of uncomfortable situations for service providers.

Comparison

The two instruments present significant similarities. They are two instruments with the same or similar purpose: gathering evidence using mutual recognition of orders of other member states. They have the same legal basis: Art. 82 (1) TFEU. Yet, while EIO is a classical mutual recognition instrument, the EPO is more controversial as it subtracts, in the regular course of events, the involvement of an authority on the receiving end of the order. In that sense, one may question whether there is still any recognition since there is no authority to actively recognise the order.⁹⁷ The involvement of judicial or equivalent authorities happens only if the service provider refuses to comply with the order. Before that we can only speak about a sort of tacit recognition.

The procedure of enforcement presents some similarities as to the conditions to issue the orders. They have to be scrutinised in view of necessity and proportionality as well as regarding availability of similar measures in national law to avoid forum shopping. Furthermore, both instruments may be issued for gathering evidence for proceedings against legal persons regardless of whether in the member state where the order is to be executed legal persons are subject to criminal liability.

But besides these resemblances, the two instruments present fundamental differences.

The need for the EIO stems from the free movement of persons and abolition of borders.⁹⁸ The reason for EPO is different, namely lack of borders in cyberspace. It is not the population that moves, but services are placed in other countries than their users. There may be need for an EPO in a purely domestic case, with perpetrators, victims, place of commission and investigating authorities all from one locality, just because the data that are needed happen to be in possession of a service provider from another member state.

In consequence, the EPO focuses much more on the relationship between the authorities seeking electronic evidence and the service providers having it. This aspect creates the major difference between the two systems. The EPO goes in the first place to the service provider who should respond to it by delivering the requested data without engaging local authorities who could exercise some checking function from the perspective of national interest or fundamental rights. Limited possibilities in that respect have been proposed by the Council with the notification procedure. However, outside of it, the primary responsibility for checking the order will lie with the service providers. Recital 46 says: ‘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’. The Council deleted the word ‘exclusively’ and added that the responsibility for the legality of the order is with the issuing authority. Furthermore, in that version, the Regulation does not offer grounds for the service provider to refuse the order, except for reasons of practical impossibility. Any refusal for potentially good but other reasons will have to be done under threat of sanctions for non-compliance. Yet, the service providers will probably perform checks anyway. The case of the San Bernardino shooter is an excellent example when a

97. Martin Böse, *An assessment of the Commission’s proposals on electronic evidence*, Study requested by the LIBE committee of the EU Parliament, 36. See also Elodie Sellier, Anne Weyembergh, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, Study requested by the LIBE committee of the EU Parliament, 31.

98. Tampere European Council 15 and 16 October 1999 Presidency Conclusions, Points 2–6.

service provider prefers to send a message to the clients: 'we protect your data' even at a risk of sanctions (and it was a terrorism case, where little sympathy could have been expected from the public towards the privacy of the deceased perpetrator).⁹⁹ Yet the logic is a different one than that of state authorities with duties to protect its citizens from violations of fundamental rights. The service providers are motivated by business concerns and their foremost duty is towards shareholders. So they will arguably respond negatively to abusive orders if that is more profitable/less damaging than complying with it.¹⁰⁰

This is not at all the case for EIO even when requiring cooperation of private actors. The EIO always passes through the hands of a competent authority entitled to perform necessary checks. In particular, EIO contains a significant list of grounds for refusal, including the fundamental rights one. The latter has been deleted by the Council in the e-evidence Regulation. While the proposed Regulation still contains the general fundamental rights clause (Art. 1 (2) EPOR), its use will rather be exceptional. The overall list of grounds for refusal is much shorter omitting for instance double-criminality, which is completely abandoned. That means for instance that a member state with very liberal abortion laws will have to enforce orders related to draconian anti-abortion policies. In sum, even if the enforcement phase of EPO is similar to the EIO, in essence the space for intervention of the enforcing authority is lesser than that of the executing authority of the EIO (even in the Council's version including notification procedure). In consequence, the EPOR requires a much more significant trust between member states than classical mutual recognition instruments such as EIO or EAW.

Necessarily, these design features will have its bearing on the rights of the person affected by the measure, be they accused or suspects, or just third parties. The service providers will be the first guardians of their rights. But when assessing their potential infringements, instead of looking at them with a public eye, they will do so with the private one. In other words, business interests will guide these assessments: what is more profitable, comply with the order or resist? And even if the service providers question the orders, the possibilities of refusal of enforcing authorities will be more limited than those available to executing authorities.

The initial problem of the e-evidence question was how to get data for local investigation where only the happenstance of the data being elsewhere makes the case international. It seems reasonable to be satisfied that in such cases the state of the investigation would be also responsible for procedural fairness. The Regulation mandates the member states to provide for effective remedies leaving the details to national legislation. It remains to be seen how these remedies are elaborated. But in a system designed in this way, it is questionable if one can really speak of effective remedies where a person may be subject to investigation (including collection of the content of his or her email correspondence) in another member state, in another language, and potentially not knowing about the transfer of data.

Finally, another difference between the EIO and EPO is worth underlining. The EPO is being introduced by a regulation, while the EIO was introduced through a directive. This aspect should

99. <https://www.washingtonpost.com/gdpr-consent/?destination=%2fworld%2fnational-security%2ffbi-has-accessed-san-bernardino-shooters-phone-without-apples-help%2f2016%2f03%2f28%2fe593a0e2-f52b-11e5-9804-537defcc3cf6_story.html%3f&utm_term=.07bb1dd0f0a2>.

100. This issue will arguably be linked with transparency of the procedure. In that respect, the EPOR provides monitoring and reporting duties in Art. 19.

create more homogeneity in the system, however a number of important aspects – in particular sanctions and remedies – are left to the member states' legislations.

Delimitation of the scope

Electronic evidence as defined by the EPOR is not the only electronic evidence there is. In fact, the EPOR applies to gathering of electronic evidence if a certain context and if a number of conditions apply. If adopted, EPOR will be the default instrument to gather this type of evidence, and its application will arguably be broad. However, there may be two types of reasons for it not to apply: geographical and questions of context or conditions of applicability of EPOR, leaving ground to EIO or even, in fewer instances, to other instruments of cooperation.

From the geographical point of view, the division of scope may/will be more complicated regarding three member states with limited participation in the AFSJ, namely Denmark, Ireland and the United Kingdom. As to the latter, it is unclear at this point what the status of this country will be. Even if it leaves the EU, it may still cooperate in some instruments belonging to the AFSJ, but speculating on that would be premature. In any case, UK firms offering services into the EU will have to designate a legal representative in the EU for the purposes of responding to EPO. The United Kingdom is part of the EIO, so if it stays in the EU, but does not opt-in to the Regulation, this will be the only instrument of cross-border exchange of evidence, including electronic evidence.

The contrary is possible as to Ireland. Ireland is not part of the EIO but seems to be willing to opt-in to the Regulation.¹⁰¹ This would mean that gathering of electronic evidence under the conditions analysed above would happen according to the regulation. As to any other evidence, it would need to be gathered through means offered by the 1959 MLA Convention of the Council of Europe, as Ireland is not even part of the EU 2000 MLA Convention.¹⁰² This creates certain imbalance in gathering of evidence regarding for instance persons who reside in Ireland, but are under investigation in other member states. Yet, this imbalance should not be exaggerated as electronic evidence regarding these persons may well be held by providers not located in Ireland. What is more important, this country is one of the most favoured by technological companies in Europe and may be chosen as the place for the EPO to be addressed. It is interesting to note that Ireland is also one of the countries, which allow their service providers to share data voluntarily with foreign law enforcement.¹⁰³ This would remain an option if this country does not opt in eventually. As Ireland is part of the FD on freezing orders, if it does opt-in to the EPOR, duality (as for all the other 25 member states fully participating in the AFSJ) would exist between freezing orders and the European Preservation Orders.

The difficulties of not being part of the regulation may well be exemplified by the case of Denmark. It is not bound by the EIOD, but it is part of the EU 2000 MLA Convention so this instrument remains the default option for gathering evidence with this country. By virtue of the

101. Ireland took part in the elaboration of the General Approach. The intention was also declared by the Minister for Justice and Equality as an answer to a parliamentary question on 19 June 2018, <<http://www.justice.ie/en/JELR/Pages/PQ-19-06-2018-231>>.

102. <https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCou.aspx?CountryId=293>.

103. Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 22 May 2017, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf>, 1.

annex to Protocol 22 to the TFEU, it may still become part of the Regulation, yet its record does not show much enthusiasm in joining initiatives pertaining to the AFSJ.¹⁰⁴ If Denmark is not part of this instrument, it will still be automatically part of the Directive. The latter is based on common market provisions of Arts 53 and 62 TFEU and the exclusion of Protocol 22 does not apply to it. This will create a peculiar situation. Denmark will be obliged to implement the Directive. Furthermore, it will be possible to declare that for the purposes of receiving requests the service provider's seat is, say, in Copenhagen. The service provider (except purely local ones) would hence be obliged to comply with EPOs, but Danish authorities would not provide enforcement or sanctions for non-compliance. The only option would be to impose sanctions in the issuing member state. Paradoxically, the Regulation would in a way have some application on the territory of Denmark, but without participation of this country in the instrument.

This would indeed create a *géométrie variable* of a higher level, certainly systemically unfortunate. It would also remain a question whether Denmark could forbid (e.g. through data protection rules) local service providers from sharing data with non-Danish law enforcement outside of the MLA procedures. This could infringe the principle of sincere cooperation, yet regarding an instrument in which the member state does not participate.

The scope of application of the EPO will also be limited by the context. EPO in its current form can only be issued for criminal proceedings (and possibly for execution of certain sentences). The application of EIO is broader as it includes also two types of proceedings which do not belong to this category (see Art. 4 (b) and (c) EIOD). Electronic evidence needed for these proceedings may be gathered through EIO only.

This latter aspect is linked with the speciality principle that the Council's version of the proposal adds. If accepted, this provision will limit the use of electronic evidence, besides the proceedings for which it was gathered, to proceedings for which the EPO could have been issued or 'for preventing an immediate and serious threat to public security of the issuing State or its essential interests'.¹⁰⁵

Another significant aspect, which may limit the application of EPO – in comparison to EIO – is the authority to issue an order. The main difference between the two instruments is that the regulation harmonises the question who may issue an EPO, while EIO leaves it to the member states. In this harmonised framework, the power of prosecutors to issue an EPO is limited (e.g. in respect of orders concerning transactional or content data). However, it is not excluded that national law permits the prosecutors to request data of that kind on the national level. In result, in such situations a prosecutor would be entitled to issue an EIO without a judge's approval, while the issuance of an EPO would necessitate such approval. However, this effect may be mitigated by the potential requirement of court authorisation in the executing member state.¹⁰⁶

104. See the list of the instruments applying to Denmark on the webpage of the European Judicial Network. <https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCou.aspx?CountryId=260>

105. Article 12b EPOR.

106. Article 2 (d) last sentence EIOD. In the judgment of 27 May 2019 in joined cases C-508/18 and C-82/19 PPU (ECLI: EU: C:2019:456), the Court considered German prosecutors not to be suitable as 'issuing judicial authority' in the context of the European Arrest Warrant, as they are 'exposed to the risk of being subject, directly or indirectly, to directions or instructions in a specific case from the executive, such as a Minister for Justice, in connection with the adoption of a decision to issue a European arrest warrant'. The applicability of this approach to other mutual recognition instruments is unclear so far (see on that also the Opinion of the AG Campos Sánchez-Bordona in that case at 37). In its judgment of 12 December 2019 in joined cases C-566/19 PPU, C-626/19 PPU and C-627/19 PPU (ECLI:

Besides these situations, competent authorities gathering electronic evidence (in the broad, non-EPOR sense) will have both instruments at their disposal (EPOR does not preclude the application of the EIOD). Yet, the application of EPO may still be limited by the fact that this evidence must be stored by or on behalf of a service provider as defined in Art. 2 (3) of the Regulation. More importantly, this must be so at the time of reception of the order. EPdO to produce transaction or content data may only be issued for certain types of offences prescribed by the regulation. Again, the question for which offences an EIO may be issued is left for the member states, so solutions may differ in different issuing states. Hence, it would still be possible to issue an EIO for transactional or content data for offences which are out of the scope of the EPdO, if the law of a member state so allows.

Systemic consequences

If both instruments are available, it is difficult to imagine why authorities should not choose an EPO. Its procedure is simpler, the deadline for reaction much shorter and the pressure on execution much more significant with a set of concrete sanctions. And if the service provider does not provide the requested data, a procedure similar to EIO is still available, but again less cumbersome (i.e. less grounds for refusal). The first potential systemic consequence, potentially with an Orwellian reminiscence, is that this may create a tendency to generally prefer electronic evidence and increasingly build up cases around it.

Is there a good reason to single out digital evidence and provide for such a facilitated system? The standard answer is that volatility of data demands celerity. Yet not only electronic evidence may require rapid access to information. A search may be urgently necessary in a kidnapping case. And it is not so that urgency is always needed when looking for digital evidence. In the name of celerity, a significant level of protection is sacrificed that is deemed necessary otherwise. Moreover, an EPO can constitute a very significant curtailment of the right to privacy, for instance if content of private emails is concerned. Much less intrusive measures (e.g. production request for company documents) are subject to a much higher level of protection as offered by EIOD. This does not contribute to systemic coherence.

From a different perspective, one may say that the EPOR finally takes mutual recognition in particular, and the AFSJ in general, seriously. Mutual recognition has been a device facilitating transnational cooperation in criminal matters for the past 20 years, which has been designed to respond to the needs of law enforcement resulting from the design of the EU. While it proclaimed trust, it always kept ways of checking if other member states are worth that trust. EPO requires a much higher level of trust and in this sense is a quantum leap of mutual recognition.

Yet it comes without full harmonisation of procedural guarantees, remedies and other elements that could substantiate it. The EU successfully built a common data protection framework, but the approach to privacy is not the same.¹⁰⁷ Furthermore, some member states are under scrutiny for

EU: C:2019:1077), the Court seems to be softening its stance in that respect. This controversy, which issued in the context of deprivation of liberty, is necessarily less acute in the context of gathering of evidence.

107. See for instance the controversy regarding implementation of the GDPR in Romania. <<https://privacyinternational.org/blog/2456/teleormanleaks-explained-privacy-freedom-expression-and-public-interest>>.

their potentially unsatisfactory level of the rule of law, which stalemated the execution of classical instruments of mutual recognition.¹⁰⁸

Finally, the EPOR creates a new relationship between law enforcement and private actors, that is, service providers, which, whether they like it or not, would become extended arms of law enforcement replacing their national authorities in the task of not only receiving and complying with but also assessing the orders. However, contrary to national authorities, they will do so at a threat of sanctions for non-compliance, making the service providers unreliable defenders of our fundamental rights.¹⁰⁹

Conclusions

The analysis above showed that if the EPO is applicable, it is much more attractive for law enforcement than EIO. It will thus become the preferred option for authorities probably increasing the presence of digital evidence in the file, potentially unnecessarily. At the same time, the EPOR is less protective for persons concerned. By giving electronic evidence preferential treatment, not only does the EPOR risk creating imbalance in the EU system of cross-border gathering of evidence but also giving up fundamental rights protection for the sake of celerity.

Furthermore, with EPOR the trust the member states have to have in each other's systems in general, and authorities' restraint in particular, is heightened to a new level: the authorities in the member state where the order is addressed being potentially completely omitted from the process and even if they intervene, they have limited grounds for opposing the order. And this development comes at a time, when mutual trust is questioned with increased intensity.¹¹⁰

EPOR has also significant merits. In the first place, it breaks with the traditional and cumbersome territorial approach to the location of data and adapts to the borderless reality of the cyberspace. Secondly, if it manages to contribute to establishing a common framework of voluntary exchange of evidence with the United States, that will certainly enhance coherence of the AFSJ. Finally, one may acknowledge the potential effect of alleviating law enforcement – which is always struggling from limited resources – from the task of reception, recognition and execution of potentially numerous orders for electronic evidence. In that way, EPOR is part of a wider trend of transferring enforcement tasks to private actors.

With the EIO, the AFSJ was supposed to get a single instrument to transfer evidence across borders of its member states.¹¹¹ Just after its implementation date, and before the practice of its use is established, a new instrument threatens to shatter this holistic approach. Instead of always having recourse to an EIO, law enforcement will have to choose between EIO and EPO and wherever possible will most likely choose EPO. While all evidence was supposed to be equal within the AFSJ, electronic evidence with its significantly simplified framework becomes more equal than any other.

108. As is the case for Poland after the case of C-216/18 PPU – Minister for Justice and Equality. See on that Petra Bárd, Wouter van Ballegooij, 'Judicial Independence as a Precondition for Mutual Trust? The CJEU in Minister for Justice and Equality v. LM' (2018) 9 NJECL, 353–365.

109. Valsamis Mitsilegas, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence' (2018) 25 *Maastricht Journal of European and Comparative Law* 3, 263–265, 264 f.

110. See an analysis of this trend by Auke Willems, 'The Court of Justice of the European Union's Mutual Trust Journey in EU Criminal Law: From a Presumption to (Room for) Rebuttal' (2019) 20 *German Law Journal* 468–495.

111. Recital 7 EIOD.


Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Stanislaw Tosza  <https://orcid.org/0000-0002-3265-1460>