Article

NJECL

New Journal of European Criminal Law
2024, Vol. 15(3) 256–274

DOI: 10.1177/20322844241258649
journals.sagepub.com/home/nje
Sage

Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation

Athina Sachoulidou
Aristotle University of Thessaloniki, Greece
Universidade NOVA de Lisboa, Portugal

Abstract
As the 'cyber' element infiltrates a significant part of criminal activity, the significance of accessing electronic evidence has risen to a critical level. The storage of this evidence outside the investigating jurisdiction prompted law enforcement authorities to actively explore avenues for collaboration with private service providers on a voluntary basis. This has resulted in the establishment of an informal channel of cooperation, running parallel to those established through mutual legal assistance and the principle of mutual recognition. The EU legislator has recently formalised this type of cooperation by adopting the Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence, along with the Directive (EU) 2023/1544. This article provides a comprehensive overview of the key provisions of this Regulation and reflects critically on the paradigm shift the latter seems to expand with respect to the privatisation of law enforcement tasks.

Keywords
electronic evidence (e-evidence), European Production Order (EPO), European Preservation Order (EPO-PR), service providers, principle of mutual recognition

Corresponding author:
Athina Sachoulidou, Assistant Professor in Criminal Law, School of Law, Aristotle University of Thessaloniki, Greece; Visiting Senior Researcher, CEDIS, NOVA School of Law, Universidade NOVA de Lisboa, Portugal.
Emails: sachoulidou@law.auth.gr; athina.sachoulidou@novalaw.unl.pt

Introduction

The widespread use of online services to achieve criminal purposes that often go beyond the commission of classic cybercrimes (cyber-dependent or -enabled crimes)[1] has stressed the urgent need for continuous modernisation and adaptation of the toolkit police and judicial authorities use at national and trans-national level. In particular, access to electronic data (also known as digital data, a term that includes distinct data categories, such as subscriber data, traffic data and content data in the field of telecommunications)[2] is an integral part of the timely prevention and effective suppression of modern criminal activity.[3] This can be achieved in different ways depending on the applicable law in the jurisdiction where the electronic data is stored and the existence of bilateral or international agreements on cross-border access to electronic data or evidence in general, but also on the basis of additional parameters such as whether the data in question is open access.

In practice, however, access to electronic data by competent authorities is a fairly complicated matter. The primary reason is the length of the procedures set out in the available mutual legal assistance instruments that –despite aiming at tackling cybercrime and, thus, taking into considering the specificities of the respective criminal proceedings– were either adopted before the widespread use of cloud computing (e.g., Budapest Convention) or –although they address cross-border access to evidence in criminal proceedings– they do not include specialised rules on electronic data given their short life-cycle (e.g., European Investigation Order (hereinafter EIO) Directive).[4] Thus, while the EIO Directive was adopted on the basis of the principle of mutual recognition of judgments and judicial decisions[5] and established a channel of *cooperation between the competent authorities of Member States* for the purpose of carrying out investigative measures, access to electronic data is often ultimately secured through *voluntary, direct cooperation between foreign service providers*

1. On the definition of the term 'cyber-crime' and the typologies suggested in the scholarship see Jonathan Clough, *Principles of cybercrime* (2nd edn, CUP 2015); *id*., 'Cybercrime' in Pedro Caeiro, Sabine Gless, Valsamis Mitsilegas, Miguel João Costa, Janneke De Snaijer and Georgia Theodorakoupoulou (eds) *Elgar Encyclopaedia of Crime and Criminal Justice* (Elgar 2024).
2. See Council of Europe, Convention on Cybercrime (hereinafter 'Budapest Convention'), art. 18 (3) (subscriber data) and art. 1 lit. d (traffic data); *id*., Explanatory Report to the Convention on Cybercrime (2021) <https://rm.coe.int/16800cce5b> accessed 21 January 2024, para. 209 (content data). Similar typologies are included into the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, art. 2. On the lack of harmonisation of national legislations on electronic data as evidence in criminal matters, including the definition of the respective terms, see EVIDENCE Project – European Informatics Data Exchange Framework for Courts and Evidence, 'D3.1 Overview of existing legal framework in the EU Member States' (2015) <https://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf> accessed 21 January 2024, 64–71; Nathalie Smuha, 'Towards the EU harmonization of access to cross-border e-evidence: Challenges for fundamental rights & consistency' (2018) European Criminal Law Review, 83 *et seq*.
3. See Claudia Warken, 'Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1. Beweissicherung im Zeitalter der digitalen Cloud' (2017) NZWiSt, 289 (290–291).
4. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
5. On the function of the principle of mutual recognition in the realm of EU criminal law see Valsamis Mitsilegas, *EU Criminal Law* (2nd edn, Hart Publishing 2022) 196 *et seq*.

and national law enforcement and judicial authorities.[6] Being faster and less bureaucratic,[7] this alternative has indeed become a popular practice compared to the use of mutual legal assistance tools, although it does not always guarantee the successful outcome of the cooperation requests.

In particular, according to a Europol study, direct cooperation with foreign service providers is not regulated (at least not explicitly) in the majority of the EU Member States.[8] This results in different treatment of the cooperation requests submitted by national authorities depending on the location of the service provider's establishment. Moreover, pursuant to the same study, it remains uncertain whether the data obtained by means of voluntary cooperation will be admissible as evidence before the competent national criminal courts.[9] The cooperation of service providers cannot be taken for granted either. There are varying reasons, including conflicting national legislations that raise questions about the legality of cooperation with foreign police and judicial authorities, the lack of resources to address an increasing number of requests as well as the lack of willingness to establish cooperation protocols for this purpose.[10]

In this context, the new EU legislation on cross-border access to electronic evidence (hereinafter 'e-evidence') in criminal proceedings appears to be a major breakthrough. This was adopted in July 2023 after complex and lengthy negotiations[11] following the release of the Commission's Proposal in April 2018.[12]

6. See Europol, 'SIRIUS EU Electronic Evidence Situation Report' (2023) <https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2023> accessed 21 January 2024, 15; Commission, 'Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward' (2017) <https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf> accessed 21 January 2024, 3.
7. See the respective empirical data at Europol, 'SIRIUS EU Digital Evidence Situation Report. Cross-border access to electronic evidence' (2019) <https://www.europol.europa.eu/cms/sites/default/files/documents/siriuseudigitalevidencereport.pdf> accessed 21 January 2024, 15; 17; 22; *id*., 'SIRIUS EU Digital Evidence Situation Report. 2nd Annual Report' (2020) <https://www.europol.europa.eu/cms/sites/default/files/documents/siriusdesr2020.pdf> accessed 21 January 2024, 25; 38–39; *id*., 'SIRIUS EU Digital Evidence Situation Report. 3rd Annual Report' (2021) <https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUSDESR122021.pdf> accessed 21 January 2024, 40; 49; 51; *id*., 'SIRIUS EU Digital Evidence Situation Report' (2022) <https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUSDESR2022.pdf > accessed 21 January 2024, 50; *id*. (n 6) 31; 59.
8. See the comparative data at Europol (n 6) 37 *et seq*.
9. See the comparative data at Europol (n 6) 42.
10. See Europol (n 6) 16.
11. For an overview of the major challenges that arose during the negotiations see Gianluca Forlani, 'The E-evidence Package. The Happy Ending of a Long Negotiation Saga' (2023) eucrim 2, 174 *et seq*.
12. Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD) (hereinafter 'Commission's Proposal') <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52018PC0225> accessed 21 January 2024; 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, COM/2018/226 final - 2018/0107 (COD) <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52018PC0226> accessed 21 January 2024. For a critical reflection on the contents of these proposals see, among others, Martin Böse, 'An assessment of the Commission's proposals on electronic evidence' (2018) <https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2018)604989> accessed 21 January 2024; Theodore Christakis, 'From Mutual Trust to the Gordian Knot of Notifications. The EU E-Evidence Regulation and Directive' in Vanessa Franssen and Stanislaw Tosza (eds) *The Cambridge Handbook of Digital Evidence in Criminal Matters* (in press, CUP) <https://papers.ssrn.com/sol3/papers.cfm?abstractid=4306874> accessed 21 January 2024, 4 *et seq*.; Vanessa Franssen, 'The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?' (2018) European Law Blog <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> accessed 21 January 2024; and Christoph Burchard, 'Europäische E-Evidence-Verordnung. Rechtsstaatlich defizitär, der Realität hinterher und langfristig konträr zu europäischen Interessen' (2019) ZRP 52, 164 *et seq*.

The new rules are entailed in the Regulation (EU) 2023/1543 (hereinafter 'the Regulation')[13] and the Directive (EU) 2023/1544 (hereinafter 'the Directive')[14] and will enter into force in August 2026.[15] The Regulation leads to (or rather extends) a *paradigm shift*[16] towards facilitating direct cooperation between competent national authorities and foreign service providers operating in the EU, regardless of the location of their establishment and, thus, their direct involvement in law enforcement. At the same time, the Directive ensures that service providers offering services in the EU, without having an establishment within the EU borders, will appoint a legal representative in at least one EU Member State for the purpose of preserving and producing e-evidence in criminal proceedings.

This article provides a comprehensive overview of the key provisions of the Regulation (Section II).[17] Next, it reflects critically on the central legislative decision to regulate direct cooperation with service providers in terms of a paradigm shift that (further) promotes the privatisation of law enforcement tasks (Section III), as well as on other normative choices that seem to prioritise speed and effectiveness of criminal repression at the expense of the protection of fundamental rights (Section IV). Lastly, it discusses future challenges that arise not only from the future enforcement of this new EU legislation but also from rapid technological developments that enable, *inter alia*, the direct generation of evidence from information systems (Section V).

Key legislative choices in the context of the Regulation (EU) 2023/1543

Justification and scope of application

The new EU legislation on cross-border access to e-evidence was adopted with a twofold goal: *first* (and foremost), to enhance the efficiency of police investigations and crime prosecution and to strengthen confidence in the digital single market through improving security and reducing the sense of impunity for crimes committed in online settings and, *second*, to improve the protection of fundamental rights of those affected by such cross-border investigations. Thus, the new tools it

13. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (hereinafter 'Regulation (EU) 2023/1543').
14. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (hereinafter 'Directive (EU) 2023/1544').
15. For a comprehensive overview of the key provisions of *both* legal instruments see Adam Juszczak and Elisa Sason, 'The use of electronic evidence in the European Area of Freedom, Security and Justice. An introduction to the new EU package on e-evidence' (2023) eucrim 2, 182 *et seq*.
16. See Stanislaw Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors' (2021) Computer Law & Security Review 43, 1 (2; 9).
17. Although this article discusses only the new EU e-evidence package, the adoption of the latter has coincided with four other important developments in the same area: 1) the adoption of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (see Kristin Pfeffer, 'Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln. Aktuelle nationale, europa- und völkerrechtliche Entwicklungen' (2023) eucrim 2, 170 (172); Forlani (n 11) 178–179); 2) the re-launch of the EU-US negotiations with the purpose of signing a bilateral agreement on cross-border access to e-evidence in March 2023 (see Theodore Christakis and Fabien Terpan, 'EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options' (2021) International Data Privacy Law 11, 81 *et seq*.); 3) the enforcement of the Digital Services Act (Regulation (EU) 2022/2065), which establishes minimum requirements on information requests addressed to service providers pursuant to EU Member States' domestic laws; and 4) the international negotiations on the adoption of a new UN Convention on cyber-crime which will also include rules governing international cooperation through extradition and mutual legal assistance (see Pfeffer (n 17) 172–173).

introduces, the European Production Order (hereinafter 'EPO')[18] and the European Preservation Order (hereinafter 'EPO-PR')[19] may be issued not only at the initiative of the competent authority of a Member State[20] but also at the request of a suspect or an accused person or of a lawyer on that person's behalf 'within the framework of *applicable defence rights* in accordance with national criminal procedural law'.[21] EPOs and EPOs-PR may be issued only in the framework of criminal proceedings and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, which must have been imposed by a decision that was not rendered *in absentia* (given the divergent national legal approaches to the matter),[22] in cases where the person convicted absconded from justice.[23] Furthermore, considering the lack of a harmonised approach to punishment of legal persons for criminal offences among the EU Member States, it is clarified that EPOs and EPOs-PR may be issued 'in proceedings relating to a criminal offence for which a legal person could be held liable or punished in the issuing State'.[24] Lastly, the Regulation will not apply to proceedings initiated as part of mutual legal assistance to another Member State or a third party.[25]

Service providers and e-evidence: Definitions and major distinctions

The service providers, with whom the competent authorities of the issuing State[26] will cooperate directly, are defined as natural or legal persons providing electronic communication, internet domain and IP numbering and other information society services that enable user communication, storage or other processing of data on behalf of the user.[27] Using criteria known in the realm of private law (e.g., art. 17 (1) lit. c Regulation (EU) 1215/2012) and data protection law (e.g., art. 3 (2) lit. a General Data Protection Regulation), the link connecting the service provider and the enforcing State[28] is not the storage of the data intended for production or preservation but the provision of services in the Union.[29] This means that the EPOs and the EPOs-PR are not based on the territoriality principle, a choice justified given the complexities inherent in the principle's application in the area of access to electronic data and their volatile location. This solution has already been adopted by national legislators – with art. 39*bis* (3) of the Belgian Code of Criminal Procedure being the most representative example. The latter links the service provider's duty to allow access to

18. Regulation (EU) 2023/1543, art. 3 nr. 1.
19. Regulation (EU) 2023/1543, art. 3 nr. 2.
20. Regulation (EU) 2023/1543, art. 1 (1).
21. Regulation (EU) 2023/1543, art. 1 (2), emphasis added.
22. Regulation (EU) 2023/1543, recital 26.
23. Regulation (EU) 2023/1543, art. 2 (2).
24. *Ibid*.
25. Regulation (EU) 2023/1543, art. 2 (4). In that sense, the scope of application of the Directive (EU) 2023/1544 is broader (art. 1 (2)).
26. On the definition of the issuing authority see Regulation (EU) 2023/1543, art. 3 nr. 15 and art. 4.
27. See Regulation (EU) 2023/1543, art. 3 nr. 3. Financial services as defined in art. 2 (2) point b Directive 2006/123/EC are exempted.
28. On the definition of the enforcing State see Regulation (EU) 2023/1543, art. 3 nr. 16.
29. See Regulation (EU) 2023/1543, art. 2 (1).

electronic data not to the location of their establishment or that of data storage but to factors such as the language of the services provided, the top-level domain (.be) and the provision of local advertising.[30] Similarly, the Regulation requires that natural or legal persons in a Member State should be able to use the aforementioned services and that there is a *substantial* connection to that State.[31] This connection exists where the service provider has an establishment[32] in a Member State or –in the absence thereof– there is a significant number of users of the services it offers in one or more Member States or there is targeting of activities towards one or more Member States considering all relevant parameters, such as the use of the language or the currency of the State concerned.

Equally important is the definition of e-evidence[33] and, particularly, the distinction between the different data categories that fall into this definition's scope. With this regard, the contents of the Regulation reflect the criticism against the initial choice of the Commission's Proposal's drafters to introduce a new distinction between subscriber, access, transaction and content data.[34] This choice did not comply with already applicable international and EU legislation (e.g., Budapest Convention and Directive 2002/58/EC) and the jurisprudence of the Court of Justice of the EU (hereinafter 'CJEU'),[35] where the term 'traffic data' is used, and, thus, jeopardised horizontal consistence of EU law.[36] The Regulation reinstates, instead, the (classic) distinction between subscriber, traffic and content data, putting the focus on the realm of telecommunications.

The first category (subscriber data) includes data held by the service provider that is related to the subscription to its services, namely data that pertains to the subscriber's or customer's identity, the type of service and its duration as well as data related to the validation of the use of service, excluding means of verifying the user's identity, such as passwords.[37] Traffic data is related to the provision of a service and provides context or additional information about it (e.g., the location of the device, date, time, duration etc.).[38] Content data is defined as any digital data (e.g., text, voice video) *other than* subscriber or traffic data.[39] As will be shown below, the Regulation sets out two different regimes: one offering greater flexibility for subscriber data and data requested *solely* for the purpose of user identification *in a specific criminal investigation*, such as IP addresses and, where necessary, source ports and time stamps,[40] (deemed less intrusive) and another stricter regime for traffic data that is not solely requested for user identification purposes and content data (deemed more intrusive).

30. See *Smuha* (n 2) 93–94; Vanessa Franssen, 'The Belgian Internet Investigatory Powers Act – A model to Pursue at European Level' (2017) EDPL 3, 534 (538–539); Stanislaw Tosza, 'The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?' (2023) EDPL 2, 163 (165). On the case of the German approach to the matter see Dominik Brodowski, 'Die "Login-Falle" zur Identifizierung von Beschuldigten im Internet – eine "grundsrechtsschonende und freiheitsorientierte" Ermittlungsmaßnahme?' (2022) Strafverteidiger, 413 *et seq*.; as to the broad interpretation of national provisions to ensure access to e-evidence see also Pfeffer (n 17) 170.
31. Regulation (EU) 2023/1543, art. 3 nr. 4.
32. On the definition of 'establishment' see Regulation (EU) 2023/1543, art. 3 nr. 5 and Directive (EU) 2023/1544, art. 2 nr. 5.
33. Regulation (EU) 2023/1543, art. 3 nr. 8.
34. See Commission's Proposal (n 12) art. 3 nr. 7–10.
35. See, for instance, CJEU, Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland), ECLI:EU:C:2014:238; *id*., Case C-623/17 (Privacy International), ECLI:EU:C:2020:790; and *id*., Joined Cases C-511/18, C-512/18 and C-520/18 (La Quadrature du Net), ECLI:EU:C:2020:791.
36. See Böse (n 12) 20; Christakis (n 12) 10.
37. Regulation (EU) 2023/1543, art. 3 nr. 9.
38. Regulation (EU) 2023/1543, art. 3 nr. 11.
39. Regulation (EU) 2023/1543, art. 3 nr. 12.
40. Regulation (EU) 2023/1543, art. 3 nr. 10.

European production and preservation orders: issuing, notification and enforcement requirements

The distinction between different data categories (see above) has a horizontal impact on several matters of regulation. First, the category of data to be *produced* determines which authority is entitled to issue such an order under art. 4 of the Regulation. Thus, EPOs to obtain subscriber data or data requested for the sole purpose of identifying the user and EPOs-PR will be issued by a judge, a court, an investigating judge *or a public prosecutor* or any other competent authority acting –in the case concerned– as an investigating authority in criminal proceedings with competence to order the gathering of evidence; in the latter case, the EPO/EPO-PR shall be validated by a judge, a court, an investigating judge *or a public prosecutor*.[41] But in those cases where traffic data (excluding data requested for the sole purpose of identifying the user) or content data are requested for production, the public prosecutor is not listed as a possible issuing authority,[42] following the CJEU jurisprudence on the matter of European prosecution authorities' independence.[43] An additional restriction is introduced, as an EPO for obtaining traffic data (not requested solely for user identification purposes) or content data many only be issued for: criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years; and –irrespective of the penalty framework– fraud and counterfeiting of non-cash means of payment, sexual abuse and sexual exploitation of children and child pornography and attacks against information systems, *if wholly or partly committed through an information system*; and, lastly, terrorist offences, *regardless of how they were committed*; and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that has not been rendered *in absentia*.[44] Such limitations do not apply to EPOs to obtain subscriber data or data requested for the sole purpose of user identification,[45] nor to EPO-PRs irrespective of the data category in question.[46]

In general, the Regulation sets out stricter conditions for issuing an EPO than an EPO-PR. Thus, the EPO shall be, *inter alia*, necessary and proportionate to the case at hand and 'may only be issued if a similar order could have been issued under the same conditions in a similar domestic case'.[47] On the contrary, in the case of an EPO-PR, the proportionality requirement is *only* tested against the 'purpose of preventing the removal, deletion or alteration of data with a view to issuing a subsequent request for production of those data', whether by means of mutual legal assistance or via an EIO or EPO.[48]

Furthermore, the Regulation provides for *additional* conditions for issuing an EPO to obtain traffic data (excluding that requested for the sole purpose of user identification) or content data in the following cases: 1) *data protected by professional privilege under the issuing State's law*, a case in which an EPO may only be issued where the privileged professional resides in the issuing State, contact with him/her might be detrimental to the investigation, or the privileges were waived in accordance with applicable

41. Regulation (EU) 2023/1543, art. 4 (1; 3); regarding *ex post* validation in validly established emergency cases see *ibid*, art. 4 (5).
42. Regulation (EU) 2023/1543, art. 4 (2).
43. See CJEU, C-508/18 and C-82/19 PPU (Minister for Justice and Equality v OG and PI), EU:C:2019:456, para. 88 and 90; Mitsilegas (n 5) 202 *et seq*.
44. Regulation (EU) 2023/1543, art. 5 (4).
45. Regulation (EU) 2023/1543, art. 5 (3).
46. Regulation (EU) 2023/1543, art. 6 (3).
47. Regulation (EU) 2023/1543, art. 5 (2).
48. Regulation (EU) 2023/1543, art. 6 (2).

law;[49] 2) *data protected by immunities or privileges granted under the law of the enforcing State or subject (in the same State) to rules on determination and limitation of criminal liability relating to freedom of the press or freedom of expression in other media*, a case in which the issuing State may seek clarification regarding the status of such data before issuing the respective EPO or shall abstain from doing so if it finds that the data in question pertains to this special category.[50] This legislative choice is part of the effort to protect as much as possible the fundamental rights of those who may become the target of a criminal investigation because of their political, professional or even voluntary activities (e.g., members of political parties, investigative journalists, members of NGOs etc.).

In the next stage, the EPOs and EPOs-PR are transmitted via certificates that, as a rule, are addressed to a designated (or, exceptionally, any other) establishment or to a legal representative of the service provider concerned[51] and, exceptionally, to the enforcing authority.[52] In particular, the Regulation provides for a notification to the enforcing authority only in the case of EPOs issued to obtain traffic data (except for that requested for the sole purpose of user identification) or content data.[53] At the same time, though, it introduces an important exception to the enforcing authority's notification for those cases where the *issuing authority* has reasonable grounds to believe that the offence in question has been, is being or is likely to be committed in the issuing State and the person concerned resides in the latter.[54]

The notification (or the lack thereof) impacts on the time framework for the execution of an EPO certificate (hereinafter EPOC).[55] The general rule is that the service provider shall transmit the requested data at the latest within 10 days[56] or, in emergency cases,[57] 8 hours following the receipt of the EPOC.[58] These deadlines are extended ('[…] at the end of that 10-day period […] as soon as possible upon such confirmation and at the latest at the end of that 10-day period'[59] and 96 hours[60] respectively) in cases where a notification to the enforcing authority is required and depending on whether the latter has raised a ground for refusal pursuant to art. 12 or has confirmed that it does not intend to do so. The grounds for refusal of EPOs encompass the following:[61] 1) protection of the data requested by immunities or privileges granted under the law of the enforcing State or pursuant to rules on the determination or limitation of criminal liability related to freedom of press or freedom of expression in other media;[62] 2) manifest breach of a relevant fundamental right as set out in art. 6 of the Treaty of European Union (hereinafter 'TEU') and in the Charter of Fundamental Rights of

49. Regulation (EU) 2023/1543, art. 5 (9).
50. Regulation (EU) 2023/1543, art. 5 (10).
51. Regulation (EU) 2023/1543, art. 9 (1) and art. 7.
52. Regulation (EU) 2023/1543, art. 9 (2).
53. Regulation (EU) 2023/1543, art. 8 (1).
54. Regulation (EU) 2023/1543, art. 8 (2).
55. There is no specific deadline for the execution of an EPO-PR. Art. 11 (1) of the Regulation only sets out that the addressee of the respective certificate 'shall, without undue delay, preserve the data requested'. This duty shall cease after 60 days, 'unless the issuing authority confirms […] that a subsequent request for production has been issued'. In this case, the duration of this obligation can be extended by an additional 30-day period.
56. Regulation (EU) 2023/1543, art. 10 (3).
57. Regulation (EU) 2023/1543, art. 3 nr. 18.
58. Regulation (EU) 2023/1543, art. 10 (4).
59. Regulation (EU) 2023/1543, art. 10 (2).
60. Regulation (EU) 2023/1543, art. 10 (4).
61. On the procedure following the decision of the enforcing authority to raise a ground for refusal see Regulation (EU) 2023/1543, art. 12 (2–5).
62. Regulation (EU) 2023/1543, art. 12 (1) lit. a.

the EU (hereinafter 'CFR');[63] 3) violation of the *ne bis in idem* principle;[64] and 4) cases where the conduct in question does not meet the double jeopardy criterion, unless it concerns one of the offences listed in Annex IV, 'if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years'.[65]

Next, art. 16 of the Regulation sets out the procedure for the enforcement of EPOs and EPOs-PR in the event that the service provider does not comply with the respective certificate without providing reasons accepted by the issuing authority and, if applicable, the enforcing authority has not raised any of the grounds for refusal listed above.[66] In this case, the EPO becomes a 'classic' mutual legal assistance instrument and its enforcement may be denied on the following grounds:[67] the EPO has not been issued or validated by a competent authority or has not been issued for one of the offences listed in art. 5 (4) of the Regulation; *de facto* impossibility to comply due to circumstances beyond the service provider's control or because of manifest errors in the EPOC; non-availability of the data requested at the time of receipt of the EPOC; the service in question is not covered by the Regulation; the protection of data by immunities or privileges granted under the law of the enforcing State or on the basis of rules on the determination or limitation of criminal liability related to freedom of the press or freedom of expression in other media; and reasonable suspicion of a manifest breach of fundamental rights. The grounds for refusing the execution of an EPO-PR are similar.[68] Lastly, in the event of non-compliance with the obligations under a recognised EPO or EPO-PR, the enforceability of which has been confirmed by the enforcing authority, as well as in the event of breach of the execution deadlines set out in arts. 10-11 of the Regulation, the service provider will have to face significant pecuniary penalties[69] of 'up to 2% of the total worldwide annual turnover of [its] preceding financial year'.[70]

Protection of the affected individuals' fundamental rights

This Regulation facilitates the establishment of a data access framework that delves into one of the most intimate realms of privacy in the digital age: the content and context of telecommunications. Operating with a focus on speed and efficiency, this framework poses a challenge to ensuring the protection of fundamental rights. The compromise solutions agreed upon during the considerably lengthy trilogue negotiations aim to reintroduce the affected individual into the equation. This is, for instance, the case, with the –albeit exceptional– notification of the enforcing authority, the reinstatement of the compliance with the *ne bis in idem* principle and the requirement of double jeopardy as grounds for refusing to execute an EPO as well as with the possibility for the enforcing State to intervene and raise such grounds for refusal to execute an EPO or EPO-PR even in cases where no notification has taken place (see above). These steps are positive in that they reintroduce the enforcing State into the picture, enabling it to intervene and safeguard the rights of affected individuals within its jurisdiction.

63. Regulation (EU) 2023/1543, art. 12 (1) lit. b.
64. Regulation (EU) 2023/1543, art. 12 (1) lit. c.
65. Regulation (EU) 2023/1543, art. 12 (1) lit. d.
66. Cf. the review procedure in the event of conflicting obligations, arising from third countries' laws, as set out in art. 17 of the Regulation. See also Pfeffer (n 17) 171–172, who briefly presents the *status quo* of the EU-US collaboration on the matter and explains the pressing need for a bilateral agreement to overcome current obstacles.
67. Regulation (EU) 2023/1543, art. 16 (4).
68. Regulation (EU) 2023/1543, art. 16 (5).
69. Regulation (EU) 2023/1543, art. 16 (10).
70. Regulation (EU) 2023/1543, art. 15 (1).

Equally important is the user information. In particular, the issuing authority is obliged to inform – without undue delay– the person whose data is requested about the production of data on the basis of an EPO.[71] The provision of information may be delayed or restricted, or even withheld, in order to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, or to protect public and national security as well as the rights and freedoms of others.[72] In such cases, the issuing authority 'shall *indicate* in the case file' the respective reasons and the EPOC shall also include a *short* justification therefor.[73] Lastly, the Regulation provides for the affected individual's (suspect, accused person or third party) right to effective remedies against an EPO (and not an EPO-PR), a right that is to be exercised *only* before the issuing State's courts.[74]

The model of direct cooperation with service providers and the intensification of the privatisation of law enforcement

The decision of the EU legislator to formalize the previously voluntary, *direct* cooperation between the competent national authorities and foreign service providers aims to address criticism regarding the efficacy of existing mutual legal assistance instruments and, particularly, the EIO. Nonetheless, it is important to highlight that the EIO Directive is not applicable neither in Denmark, which does not participate in judicial cooperation in criminal matters at all, *nor in Ireland*, which reserves the right from participating in such instruments, as was the case with the EIO. Indeed, Ireland's decision has significantly influenced the realm of e-evidence, given that many of the most influential tech companies' European subsidiaries (e.g., Meta, Microsoft, Google) are located within the Irish jurisdiction.[75]

The model of direct cooperation entails a significant limitation on the national sovereignty of the enforcing State, where the service provider has an establishment. This limitation may comply with the Lotus principle inasmuch as it derives from an international treaty,[76] but remains a *considerably broad self-limitation* in the field of cross-border judicial cooperation in criminal matters at both EU and Council of Europe's level.[77] In particular, it is worth noting the use of an EU Regulation as a legislative instrument, which significantly constrains the national legislator's discretion in the realm of judicial cooperation,[78] and art. 82 (1) of the Treaty on the Functioning of the EU (hereinafter 'TFEU'), which serves as the central provision of primary EU law concerning judicial cooperation *among Member States* in criminal matters, as the legal basis for establishing a channel of direct cooperation *with service providers*.[79]

Pursuant to art. 82 (1) TFEU, the principle of mutual recognition serves as the basis of judicial cooperation in criminal matters at EU level. Although this provision does not ascribe a concrete meaning to the concept of mutual recognition, nor does it state that the latter necessarily refers to cooperation between national public authorities, it does certainly refer to *judicial* cooperation, a term that does not suggest the

71. Regulation (EU) 2023/1543, art. 13 (1).
72. Regulation (EU) 2023/1543, art. 13 (2) in combination with Directive (EU) 2016/680, art. 13 (3).
73. Regulation (EU) 2023/1543, art. 13 (2), emphasis added.
74. Regulation (EU) 2023/1543, art. 18 (1–2).
75. In this case, the 1959 European Convention on Mutual Assistance in Criminal Matters remains applicable. See Tosza (n 30) 164.
76. S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).
77. Tosza (n 30) 164.
78. This is, however, not a unique example. See, for instance, the 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.
79. See Böse (n 12) 36, who underlines the differences between art. 81 (2) lit. a and art. 82 (1) subpara. 2 lit. a TFEU in terms of identity and contents.

involvement of private parties.[80] Indeed, the principle of mutual recognition was 'born' in a different regulatory framework, that of European *economic* law; thus, it is often argued that it should be interpreted in a flexible way and that, in this context, there is room for taking into consideration the latest technological developments, including but not limited to the growing importance of cross-border access to e-evidence.[81] The adoption of such a view would ignore, however, the different ideological identity of European *criminal* law compared to European economic law, as in the case of the latter the application of the principle of mutual recognition enables the free movement of persons, goods and services, whereas in the case of the former it entails significant restrictions on civil liberties.[82] Besides this, this restrictive function is performed in a context that does not ensure a prior, *comprehensive* approximation of national legislations on procedural issues, including, *inter alia*, the protection of defence rights, considering that the Directives adopted on the basis of the Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings have not fully addressed this regulatory aspect.[83] In any event, it should be noted that –prior to the legislative initiative taken by the EU legislator to improve cross-border access to e-evidence– domestic legal approaches have already been fragmented regarding issues related not only to the necessary link to each national legal order for adopting investigative measures with cross-border effects *but also to the procedural guarantees* available to individuals affected by such investigative measures.[84] That said, there has already been an important (but far from being unusual) discrepancy between the gradual expansion of investigative measures and the protection of suspects or accused persons. The Regulation *does not address this matter* inasmuch as it does not delve into the exercise of the affected individuals' defence rights[85] with the exception of granting the suspect or the accused person the right to request the issuing of an EPO or an EPO-PR within the framework of applicable defence rights.[86]

It is true, however, that the cooperation with private bodies is *far from unprecedented*. The EU anti-money laundering (hereinafter 'AML') legal framework is perhaps the most representative example, considering that a significant number of due diligence duties has been imposed on private actors (the number of which has been increasing geometrically after each amendment of the AML Directives), known as obliged entities, raising questions as to the privatisation of decisions that pertain to

80. See Tosza (n 30) 169 who stresses –as a possible counterargument– that '[o]ne can accept that the recognition [of the EPO/EPO-PR] takes place tacitly, as the Member States accept that an order from another Member State enters their sovereign sphere and is executed by an obliged private actor'. Besides this, he underlines that, in case of non-compliance, the order will be turned into a mutual legal assistance instrument; that is, the enforcing State will be responsible for its execution.
81. See Tosza (n 30) 169–170, who, however, reaches a different conclusion as to the appropriateness of using art. 82 (1) TFEU as a legal basis, taking the extent to which mutual trust actually exists as a starting point.
82. Sabine Gless, 'Zum Prinzip der gegenseitigen Anerkennung' (2004) ZStW 116 (2), 353 *et seq*.; Maria Kaiafa Gbandi, *European Criminal Law and its integration into the Greek legal order* [in Greek] (Sakkoulas 2016) 28.
83. See Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, 2009/C 295/01 <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32009G1204(01)&from=ES> accessed 21 January 2024. Regarding the so-called Roadmap Directives see Mitsilegas (n 5) 254 *et seq*.
84. Council of the EU, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 15072/1/16 REV 1' (2016) <https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf> accessed 21 January 2024, 4 *et seq*. See also Smuha (n 2) 94–95. On the necessary procedural safeguards cf. Warken (n 3) 291 *et seq*.
85. Cf. Regulation (EU) 2023/1543, art. 18 (4).
86. Regulation (EU) 2023/1543, art. 1 (2).

and impact on the administration of criminal justice.[87] There are several other examples one may point out, such as the existence of *whistle-blowing* mechanisms in the private and the public sector, the operation of criminal compliance departments within private companies[88] or the so-called internal investigations to name a few.[89] This is a gradual paradigm shift that has also been confirmed by more recent initiatives of the EU legislator regarding the prevention of the dissemination of terrorist content online[90] and the monitoring of content that is made available on digital platforms[91] – with the service providers being invited to take key law enforcement related decisions, including the timely removal of illicit content online. Thus, they assume, among others, the task of striking the 'right' balance between the freedom of expression of the users of their services and other rights and interests, such as public security.[92]

In this context, it becomes apparent that the newly adopted EU legislation on cross-border access to e-evidence extends the scope of the aforementioned paradigm shift, which has already gone beyond the narrow limits of self-regulation and touched upon the sphere of the exercise of public duties, including judgments on legality, proportionality, protection of fundamental rights and so on. It has been the Commission's Proposal that first introduced the idea of privatisation of mutual legal assistance, including provisions pursuant to which the service providers would even be entrusted with the duty of examining whether the EPO at hand would manifestly violate the CFR or be manifestly abusive[93] – under the threat of sanctions to be imposed in case of non-compliance with the duties arising from the receipt of an enforceable order.[94] This scenario was not included into the Council's General Approach to the Regulation,[95] while the European Parliament also proposed the withdrawal of the provisions that set out

87. See, for instance, Valsamis Mitsilegas and Niovi Vavoula, 'The evolving EU anti-money laundering regime. Challenges for fundamental rights and the rule of law' (2016) Maastricht Journal of European and Comparative Law 2, 261 *et seq*.; Theodoros Papakyriakou, 'Criminal-law legislation on money laundering as a fundamental aspect of a new crime policy' [in Greek] in Maria Kaiafa Gbandi *et al*. (eds) *Honorary Volume for Ioannis Manoledakis*, Volume B (Sakkoulas 2007) 484 *et seq*.
88. On the function of such structures as a self-regulation mechanism in the realm of criminal law see, for instance, Athina Sachoulidou, 'Regulierung und Selbstregulierung im interdisziplinären Dialog – Die rechtliche Perspektive' (2017) Journal of Self-regulation and Regulation 3, 27 (41 *et seq*.).
89. On internal investigations as an example of privatisation of law enforcement see, for instance, Clarissa Meerts, 'The private policing of economic crime – Corporate investigations and settlements' (2023) Journal of Economic Criminology 1, 100016; Petter Gottschalk, 'Private policing of white-collar crime: case studies of internal investigations by fraud examiners' (2020) Police Practice & Research An International Journal 21, 717 *et seq*.
90. See Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
91. See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
92. See Tosza (n 16) 2–7.
93. See Commission's Proposal (n 12) art. 9 (5).
94. See Valsamis Mitsilegas, 'The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence' (2018) Maastricht Journal of European and Comparative Law 25, 263 *et seq*.; Böse (n 12) 23 *et seq*.; 41 *et seq*.; EDRi, 'EU E-evidence proposals turn service providers into judicial authorities' (2018) <https://edri.org/our-work/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/> accessed 21 January 2024; European Data Protection Board (EDPB), 'Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)' (2018) <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en> accessed 21 January 2024, 7; Tosza (n 16) 8 *et seq*.
95. Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – General Approach (hereinafter 'Council's General Approach'), 30 November 2018 <https://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf> accessed 21 January 2024.

sanctions as part of the amendments it voted for in December 2020.[96] Ultimately, the Regulation *only* provides for the notification of EPOs to obtain traffic data (excluding that intended solely to identify the user) or content data to the enforcing authority, which may invoke one of the grounds for refusal listed in art. 12, including the case of a manifest breach of a relevant fundamental right as set out in art. 6 TEU and in the CFR. This inevitably suggests that, in all other cases, it is the service provider that is expected to act as the 'first filter' for any such breaches and, accordingly, to deny the execution of the respective EPO or EPO-PR, in order to trigger the mechanism of art. 16 of the Regulation. However, if the enforcing authority reaches the opposite conclusion, namely that there has been no breach and that the order should have been executed in the first place, the service provider still faces the risk of being sanctioned according to art. 15 of the Regulation. This means that the service provider is confronted with the dilemma 'compliance or punishment', a dilemma that is also coupled with lack of expertise (in terms of assessing in which cases the issuing of an EPO or EPO-PR violates fundamental rights), tight deadlines and a large number of orders to be executed.[97] At the same time, the 'other cases', in which the enforcing State has little to no chance to intervene due to the lack of notification, may involve requests originating from an issuing State that seeks to identify vulnerable individuals, such as whistle-blowers or journalists who may be investigating a scandal of political corruption in the same State.[98]

This regulatory framework is compounded by the inherent 'nature' of service providers as private entities driven by corporate interests.[99] Private companies may often take initiatives for the sake of public interests (e.g., corporate social responsibility initiatives), when this also (or primarily) serves their public image or corporate agenda, but this does not mean that the exercise of public power can, nor should, be entrusted to them. On the contrary, the latter requires impartiality and independence, virtues that are often not in line with business interests, the pursuing of which may even suggest compliance with a potentially abusive EPO or EPO-PR, in order to avoid sanctions. This is particularly the case inasmuch as pecuniary sanctions have an adverse impact not only on the corporate budget, but also entail reputational damage and further financial losses, if, for instance, the refusal to comply with a certain order is publicly perceived as a cover-up of the offence under investigation. Furthermore, value judgments that fall within the public sphere are linked to a democratic system of accountability, while corporate staff is accountable to the company's shareholders and owners. In this context, the risk of abuse of power and the emergence of phenomena of corruption associated with the transfer of public power to the private sector is equally important.

Lastly, the choice to promote direct cooperation between competent public authorities and private service providers, which, among others, reflects a trend towards harmonisation of EU and US (Clarifying Lawful Overseas Use of Data (CLOUD) Act) legislative approaches to this matter,[100] implies a clear departure from the mutual trust lessons as encapsulated in the CJEU jurisprudence on the EU Framework Decision on the European Arrest Warrant (hereinafter 'EAW'), particularly

96. European Parliament, Report on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM (2018) 0225 – C8-0155/2018–2018/0108 (COD)) 2020 (hereinafter 'EP's Position') <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256EN.pdf> accessed 21 January 2024.
97. Similarly, Pavlos Topalnakos, 'Critical issues in the new EU Regulation on electronic evidence in criminal proceedings' (2023) eucrim 2, 200 (201).
98. See EDRi, '"e-Evidence" trilogues: what's left of fundamental rights safeguards' (2022) <https://edri.org/our-work/e-evidence-trilogues-whats-left-of-fundamental-rights-safeguards/> accessed 21 January 2024.
99. On the following thoughts see Papakyriakou (n 87) 484 *et seq*.; Tosza (n 16) 12.
100. See Jennifer Daskal, 'Unpacking the CLOUD Act' (2018) eucrim 4, 220 *et seq*.

regarding detention conditions in European prisons and the independence of the judiciary.[101] The strengthening of the service providers' role, coupled with the lack of notification to the enforcing State as a general rule, translates to a 'quantum leap' of mutual trust that has already been shaken when enforcing the EAW Framework Decision.[102] In that sense, it has been no coincidence that the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (hereinafter 'LIBE Committee') proposed tightening the conditions for execution of the orders issued by states investigated under art. 7 TEU.[103] Notwithstanding the above, the notification system as set out in the Regulation leaves little room for the enforcing authority to intervene, effectively turning service providers into *de facto* guardians of fundamental rights.[104]

[Further] Rule-of-law deficiencies in the Regulation (EU) 2023/1543

The formulations adopted in the final text of the Regulation and the normative choices those reflect are problematic on multiple levels, particularly if one compares them to the amendments proposed by the LIBE Committee before the beginning of the trilogue negotiations.[105] This is because they put a clear emphasis on crime repression and the effectiveness of law enforcement, a choice that comes at a price: poor protection of fundamental rights.[106] There is, however, a clear exception to this overall trend, namely the express recognition of the right of suspected or accused persons to request the issuing of an EPO or EPO-PR.[107]

First, as regards the conditions for issuing an EPO or EPO-PR, there is an ultimately *incomplete* link between these significantly invasive investigative measures and 'more serious criminal offences'.[108] Such a link is only reserved for EPOs to obtain traffic data (excluding that requested solely for the purpose of user identification) or content data either through the harmonisation criterion or through the mechanism of minimum maximum penalties (in this case, set at three-year custodial sentence). In practice, this means that, pursuant to the harmonisation criterion, an EPO may be issued in case of illegal access to information system, an act that, under certain

101. See CJEU, Joined Cases C-404/15 and C-659/15 PPU (Aranyosi/Caldararu), EU:C:2016:198 and *id*., Case C-216/18 PPU (LM), EU:C:2018:586, respectively. For a comprehensive presentation of this jurisprudence see Mitsilegas (n 5) 202 *et seq*.
102. Tosza (n 30) 168.
103. EP's Position (n 96) art. 9 (2a), according to which, in such a case, the service provider would be able to transmit the requested data only upon receipt of the executing authority's explicit written approval. Cf. Regulation (EU) 2023/1543, recital 64 and Forlani (n 11) 178.
104. Tosza (n 30) 170.
105. On the added value of the amendments proposed by the LIBE Committee see Athina Sachoulidou, 'The key elements of the LIBE Committee's compromise proposal on e-evidence: a critical overview through a fundamental rights lens' (2021) Global Affairs 7, 777 (785 *et seq*.) and Theodore Christakis, 'E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report' (2020) European Law Blog <https://europeanlawblog.eu/2020/01/21/e-evidence-in-the-euparliament-basic-features-of-birgit-sippels-draft-report/ > accessed 21 January 2024.
106. Cf., though, Regulation (EU) 2023/1543, art. 1 (3) subpara. 1 where it is stated that '[t]his Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in the Charter and in Article 6 TEU, and any obligations applicable to law enforcement authorities or judicial authorities in this respect shall remain unaffected'.
107. Regulation (EU) 2023/1543, art. 1 (2).
108. Cf. Regulation (EU) 2023/1543, recital 40–41. The term 'serious crime' is not defined in EU law, so the responsibility for determining its meaning ultimately lies with the national legislator. See Böse (n 12) 40; Irene Wieczorek, 'The emerging role of the EU as a primary normative actor in the EU Area of Criminal Justice' (2021) European Law Journal 27, 349 *et seq*.; Birgit Sippel, 'Guest editorial' (2023) eucrim 2, 109.

circumstances, national law may deem to be *not* worthy of punishment.[109] Based on the criterion of the penalty threshold, in several jurisdictions, the same measure may become available for crimes, such as simple theft.[110] The Regulation may reinstate the double jeopardy requirement as a ground for refusal, but its drafters (like those of the Commission's Proposal) seem to oversee that the minimum maximum penalty limitation emerges from exceptions to the double jeopardy requirement.[111] Birgit Sippel, the rapporteur appointed by the European Parliament, attempted to overcome such challenges in the report she drafted, proposing a limit of 5-year custodial sentence.[112] However, this solution is not necessarily optimal given the incomplete harmonisation of criminal sanctions across the EU Member States.[113]

Next, regarding the proportionality conditions for issuing an EPO or EPO-PR, the Regulation did not adopt the LIBE Committee's proposal concerning the equalisation of those conditions for both EPOs and EPOs-PR.[114] In fact, it was proposed to further strengthen proportionality conditions by setting out –in binding provisions– that there must be sufficient reasons to believe that a criminal offence *has been* committed and that this is sufficiently serious to justify the production or the preservation of electronic data, as well as that the latter is relevant to the investigation of the offence at hand and is related to *specific individuals directly connected thereto*. This would have clearly left cases where the offence under investigation is about to be committed or could be committed in the future outside the Regulation's scope.[115]

Notwithstanding the above, it has been the notification system that became the 'apple of discord' during the trilogue negotiations.[116] The solution adopted in the Regulation should be considered as a clear improvement compared to the *fast-track* system advocated by the Commission, under which the enforcing State would be involved practically only in case of non-compliance of the service provider,[117] *as well as* to the solution proposed by the Council, namely the solution of notifying the enforcing State (without suspensive effect) only in case of EPOs to obtain content data and only where the issuing State would have reasonable grounds to believe that the person concerned does not reside within its territory.[118] However, the current solution is clearly inferior in terms of safeguards compared to the European Parliament's intervention, as part of which it was proposed to notify the enforcing State in case of both EPOs (irrespective of the data requested for production) *and* EPOs-PR, in order to enable it to raise grounds for refusal in a timely manner – with the

109. See, for instance, Greek Penal Code, art. 370B subpara. 2.
110. See, for instance, Greek Penal Code, art. 372 (1) subpara. 1.
111. Böse (n 12) 40. Similarly, Topalnakos (n 97) 202, who stresses that, in any event, the dual criminality requirement will only apply to EPOs and to those cases where traffic data (except for those requested solely for the purpose of user identification) and content data are requested for production.
112. European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Draft report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM (2018) 0225 – C8-0155/2018–2018/0108 (COD)), Rapporteur: Birgit Sippel (hereinafter 'Sippel's report') (2019) <https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987EN.pdf> accessed 21 January 2024, 71.
113. On the issues arising from the use of minimum maximum penalties as a legislative instrument see European Criminal Policy Initiative, 'A Manifesto on European Criminal Policy' (2009) ZIS 12, 708 *et seq*.
114. EP's Position (n 96) art. 5 (2) and art. 6 (2).
115. Cf. Sachoulidou (n 105) 787. See, however, Regulation (EU) 2023/1543, recital 24 that expressly refers to a specific criminal offence that has already taken place.
116. See Christakis (n 12) 20 *et seq*.; Forlani (n 11) 175.
117. Commission's Proposal (n 12) art. 14.
118. Council's General Approach (n 95) art. 7a (1; 4).

suspensive effect of the notification varying depending on the type of the order and the type of the data requested.[119]

The notification duty introduced in art. 8 (1) of the Regulation, being a compromise solution, is of central importance to the extent that the issuing State cannot always be expected to exercise the same diligence to effectively protect the rights of those residing outside its territory (particularly where national interests dictate the need to access specific evidence), nor it can always be expected to know whether there are parallel criminal proceedings in another Member State to which there will be no notification.[120] Similarly, however, the enforcing State cannot be expected to actively support the prosecution of an act that is not typified as a crime in the national legal order, particularly in those cases that touch upon the value code of a legal order (e.g., criminalisation of abortion).[121] Nonetheless, the 'exception to the exception' envisaged in art. 8 (2) of the Regulation coupled with the criterion of residence strengthens unilaterally the position of the issuing State, considering that it is upon the latter to determine the place of residence.[122] The same State, however, has expressed – from the outset– its interest in the execution of the order in question by means of issuing it.[123]

Next, regarding the addressees of EPOs and EPO-PRs, Birgit Sippel submitted the most comprehensive proposal for the protection of the affected individual, a proposal including the notification not only of the enforcing State but also of the so-called affected State, where the affected individual resides (provided this is not the issuing State, nor the enforcing State).[124] This proposal was rejected at European Parliament's level, as it was considered to have a negative impact on the efficiency of the overall procedure.[125] Instead, the negotiating forces focused on achieving the objective of the (at least partial) involvement of the enforcing State. However, the affected individual may have limited to no connection to the State,[126] where the service provider may happen to be established due to a favourable tax regime. It should also be borne in mind that, in reality, a Member State, such as Ireland, where a large number of service providers have an establishment, will not be able to monitor closely the range of orders executed on its territory. Besides this, other Member States may hesitate to scrupulously monitor the execution of orders of purely national nature, which do not anyhow involve or affect their nationals. Thus, notifying the affected State could be crucial for the protection of the persons residing within its jurisdiction and, possibly, its national interests, should, for instance, an EPO be issued to investigate a political offence. In any event, to ensure that the efficiency of the procedure remains intact, the notification of the affected State could take place within the same time framework set by the Regulation for the execution of EPOs.[127] Lastly, it should be noted that in case that the affected State differs from the issuing State, the exercise of the right to effective legal remedies requires seeking legal advice in and getting familiar with a foreign jurisdiction.[128]

119. EP's Position (n 96) art. 7–10a.
120. See Christakis (n 12) 13; 16.
121. EDPB (n 94) 6.
122. Cf. Forlani (n 11) 178.
123. See EDRi (n 98); Athina Sachoulidou, 'Cross-border access to electronic evidence: is there any light at the end of the tunnel?' (2023) <https://trace-illicit-money-flows.eu/cross-border-access-to-electronic-evidence-is-there-any-light-at-the-end-of-the-tunnel/> accessed 21 January 2024.
124. Sippel's report (n 112) 146.
125. Cf. the criticism expressed by Christakis (n 105) as to the EP's position.
126. Christakis (n 12) 24.
127. Christakis (n 12) 22–23.
128. Cf. the other examples provided by Juszczak and Sason (n 15) 193.

The significant concentration of powers in the issuing State becomes apparent in the light of the legislative choices in two additional areas: the user information pursuant to art. 13 and the exercise of the right to effective legal remedies pursuant to art. 18 of the Regulation. The Commission's Proposal set out the possibility of not informing the affected individual if requested by the issuing authority,[129] while the Council advocated a stricter position: the rule of non-informing the affected individual unless explicitly requested by the issuing authority.[130] Instead, the LIBE Committee proposed a model of by-default provision of information (for both EPOs and EPOs-PR), from which the service provider could only refrain on the basis of a *duly justified judicial order* that would specify the duration of the confidentiality duty and would be subject to periodical review.[131] The Regulation adopts the Commission's view on this matter and, thus, strengthens the position of the issuing State by favouring the 'loose' safeguard of the 'short justification' in case of choosing to delay, limit or even refrain from providing information over the 'duly justified judicial order', a solution that could set clear limits on the circumvention of the issuing State's power to refrain from informing the affected individual.

Similarly, the exercise of the right to effective legal remedies has been concentrated in the courts of the issuing State, a choice that seems to ignore the experience of the execution of EAWs. On the contrary, the LIBE Committee's proposals adopted by the European Parliament set out the possibility to challenge the legality of the EPO/EPO-PR as well as the fulfilment of the necessity and proportionality requirements before the courts of the enforcing State too.[132] Such a solution would ensure effective judicial protection for those individuals that do not reside in the issuing State, are not familiar with this national legal order, nor speak its language.[133] In parallel, it takes into consideration the different levels of protection of the rule-of-law principles and the impact thereof on mutual trust among the EU Member States.[134] In any event, the final wording of art. 18 (2) of the Regulation '[…] without prejudice to the guarantees of fundamental rights in the enforcing State' remains rather *ambiguous* as regards its actual impact on the protection of the affected individuals.[135]

Lastly, according to art. 18 (4) of the Regulation, the issuing State (and any other Member State to which e-evidence has been transmitted under this Regulation) is obliged to 'ensure that the rights of defence and fairness of the proceedings are respected when assessing evidence obtained through the [EPO]'. This provision, however, may be turned into empty words in the absence of specific regulation that takes into account the particularities of e-evidence, given, *inter alia*, the real risk of tampering with such evidence[136] and the strong interference with the rights of suspects and accused persons or third parties that communicate with them,[137] as well as in the absence of harmonised rules

129. Commission's Proposal (n 12) art. 11 (1).
130. Council's General Approach (n 95) art. 11 (1).
131. EP's Position (n 96) art. 11 (1a).
132. EP's Position (n 96) art. 17 (1–3a).
133. See Böse (n 12) 27; Christakis (n 12) 16.
134. See Stalislaw Tosza, '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' (2020) NJECL 11, 161 (182).
135. Contrary, Topalnakos (n 97) 202–203, who argues that art. 18 (2) may 'have regulatory content that includes the review of the Order by the enforcing state when requested by the person concerned, as provided in the domestic law for the same cases'.
136. Nonetheless, it should be underlined that the Regulation provides for the creation of a decentralised IT system (art. 19 *et seq*.) aiming to ensure the safety of order and data exchanges among the EU Member States as well as that service providers receive orders only from authenticated authorities.
137. Cf. Warken (n 3) 291 *et seq*.

on the admissibility of evidence in general and e-evidence in particular.[138] The LIBE Committee's proposal included, instead, explicit provisions to the effect that electronic information obtained in breach of the Regulation would not be admissible before national courts; the same would apply to information obtained before a ground for refusal has been raised.[139] None of these provisions was adopted by the drafters of the Regulation. The latter will enter into force in 2026;[140] at this point, it should be assessed as to whether it achieves, among others, the goal of protecting the rights of the affected individuals – with national courts being 'charged' with surfacing persistent challenges and the CJEU with resolving them.

Future challenges

The EU legislator's initiative to regulate cross-border access to e-evidence in criminal proceedings[141] showcases the increasing importance of the second generation of forensic evidence, which includes, *inter alia*, digital data.[142] Its use implies the need to ensure that *citizens* become familiar with the features of such evidence as well as to create the right infrastructure for processing it, coupled with the need to provide thorough training to *members of law enforcement and criminal justice authorities*, to ensure its reliable assessment, as well to of *defence lawyers* who will either make use of art. 1 (2) of the Regulation or will be called to rebut e-evidence obtained through an EPO in criminal proceedings.

However, the lack of harmonised rules on the admissibility of (e-)evidence remains a challenge, which will become more persistent in the light of the emerging third generation of forensic evidence that will be generated *directly* by information systems.[143] While e-evidence includes, *inter alia*, content data that may be exchanged through an instant messaging application, artificial intelligence (AI)-generated evidence will include, for instance, the output of a deepfake detector that examines the authenticity of the content data mentioned above (e.g., voice mail) with the help of AI. While few jurisdictions have taken steps to regulate the use of AI-generate evidence, the EU initiatives culminated in the Proposal for a Regulation laying down harmonised rules on AI, the final text of which was adopted by the European Parliament on 13 March 2024[144]. This may have an *indirect*

138. See European Law Institute, 'ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings' (2023) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf> accessed 21 January 2024; Lorena Bachmaier Winter, 'Mutual admissibility of evidence and electronic evidence in the EU. A new try for European minimum rules in criminal proceedings?' (2023) eucrim 2, 223 *et seq*.
139. EP's Position (n 96) art. 11c.
140. As to the future implications for stakeholders, including the conflicting rules and duties of service providers, see Juszczak and Sason (n 15) 192–193.
141. As to the importance of accessing e-evidence in *punitive* administrative proceedings see Stanislaw Tosza, 'Gathering electronic evidence for administrative investigations. Exploring an under-the-radar area' (2023) eucrim 2, 216 *et seq*.
142. Cf. Erin Murphy, 'The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence' (2007) California Law Review 95, 721 *et seq*.
143. See Sabine Gless, 'AI in the courtroom: a comparative analysis of machine evidence in criminal trials' (2020) Georgetown Journal of International Law 51, 195 *et seq*.
144. European Parliament, Legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html> accessed 20 April 2024.

impact on the use of AI in the realm of criminal justice, but, certainly, does not focus on matters that pertain to procedural criminal law and evidence law in particular. This implies that criminal justice professionals, who are still adapting to the digital landscape, will soon be tasked with categorizing a new generation of evidence, the decoding of which largely rests in the hands of the private sector, presenting them with the great challenge to ensure the protection of fundamental rights.

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) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Horizon 2020 Framework Programme, 101022004.

ORCID iD

Athina Sachoulidou https://orcid.org/0000-0002-8156-6668