# Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings

**Pavlos G. Topalnakos**

eucrim
European Law Forum: Prevention • Investigation • Prosecution

## ABSTRACT

The new EU Regulation on electronic evidence in criminal proceedings not only aims to enhance cross-border access to electronic evidence but also raises concerns regarding privacy, fundamental rights, and accountability. This article focuses on three key issues.
First, it is argued that the establishment of a direct cooperation framework between the issuing state and private service providers regarding data of citizens from other Member States reinterprets Art. 82 TFEU and circumvents the traditional review and scrutiny by the judicial authorities of the enforcing state, compromising transparency and individual rights.
Second, the rules in the Regulation that eliminate the requirement of dual criminality for certain categories of electronic evidence potentially lead to the collection of data for conducts that may not be criminalized in the enforcing state. In addition, the absence of the principle of speciality allows for the unintended use of evidence acquired through cooperation.
Third, the individuals' rights to privacy and data protection are potentially violated, given that European Preservation Orders fall outside the scope of legal remedies. Moreover, the lack of explicit provisions for legal protection within the enforcing state raises concerns about the effectiveness of the remedies.
The author stresses the need to strike a balance between deepening cooperation and safeguarding fundamental freedoms. He calls for reforms to ensure robust mechanisms for contesting the legality and necessity of measures, as well as clear provisions for legal protection within the enforcing state, so that a rights-based approach within the European system established by the Regulation can be achieved.

**AUTHOR**

**Pavlos G. Topalnakos**
Lawyer

**CITE THIS ARTICLE**

Topalnakos, P. G. (2023). Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-015

Published in eucrim 2023, Vol. 18(2) pp 200 – 203
https://eucrim.eu
ISSN:

# I. Introduction

The general objective of effective investigation and prosecution of crimes has always been an essential dimension of judicial cooperation in criminal matters within the EU. In the era of technological advancement, efficient judicial cooperation must include the improvement of cross-border access to electronic evidence. This improvement was initially pursued by Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order (EIO) in criminal matters.[1] However, the collection of electronic evidence through the EIO only focused on the identification of individuals who were associated with a specific telephone number or IP address[2] and on the interception of telecommunications with the technical assistance of the executing state[3]. As a result, it became quickly apparent that the EIO fell short of the set targets, because the procedures and timelines prescribed in the EIO proved unsuitable for electronic information,[4] which is more volatile and subject to swift and easy deletion.

In this context, three new objectives were set: [5]

- Reducing delays in cross-border access to electronic evidence;
- Ensuring cross-border access to evidence where it is currently missing by means of the EIO;
- Improving legal certainty, protection of fundamental rights, transparency, and accountability.

With this perspective in mind, and after a rather laborious process, final agreement was reached on the European Production Order and the European Preservation Order for electronic evidence in criminal proceedings.[6] This article will highlight three specific issues that are considered key in the Regulation: First, the new function seemingly attributed to Art. 82 of the Treaty on the Functioning of the European Union (TFEU) that regulates the judicial cooperation of Member States in criminal matters within the EU. Second, the application of fundamental principles that traditionally govern judicial cooperation between states. Third, the legal remedies provided to the individuals who are affected by the issued Orders.

# II. A New, Previously Unknown Function of Article 82 TFEU

The activation of Art. 82 TFEU in all cases where it was invoked as the legal basis for mutual cooperation between EU Member States led to the establishment of a stable framework involving two judicial authorities: those of the issuing state and those of the executing state. The new Regulation on electronic evidence changes this framework for the sake of a speedy collection of evidentiary material, bypassing the judicial authorities of the enforcing state and allowing direct cooperation between the competent authorities of the state issuing the European Production and Preservation Order and the private sector service providers. In essence, this process allows the authorities of the issuing state to gain direct access to a range of data concerning citizens of other Member States without being subject to scrutiny by the judicial authorities of the enforcing state regarding the conditions for issuing and the overall legitimacy of said Orders. It is worth emphasizing that the granted access may even cover sensitive personal data,[7] while the power of review lies primarily with the service providers, who, obviously, cannot guarantee the protection of the rights of the individuals affected by these Orders. Moreover, the protection of rights becomes even more precarious when two additional factors are taken into account: First, the execution time for the Orders is relatively short and tight, making it practically impossible to thoroughly verify the adequacy and legitimacy of said Orders.[8] Second, the threat against service providers of pecuniary sanctions for infringements of the Regulation

https://doi.org/10.30709/eucrim-2023-015

undoubtedly undermines the "will" to scrutinize the legitimacy of the Orders, as it is rather apparent that the service provider would prefer an "easy" compliance with the Orders over being subjected to the looming threat of pecuniary sanctions.[9]

The Regulation seeks to address these weaknesses by establishing, in its Art. 8, the obligation of the issuing state to inform the competent authority of the enforcing state simultaneously with the transmission of the certificate issued for the Order. However, this notification only concerns the issuance of a European Production Order, not the issuance of a European Preservation Order, and it is furthermore limited to cases where the data submitted are traffic and content data. On the contrary, cases involving data used for the sole purpose of identifying the user and subscriber data do not require notification of the enforcing state.

The characteristics of the new Regulation on European Production and Preservation Orders as described make it clear that the framework established by it, with Art. 82 TFEU as its legal basis, has fundamentally altered the essence of this provision of EU primary law, which aims to facilitate the judicial cooperation between states guided by principles of review and transparency and not between states and private entities, where critical factors, such as mutual recognition, are lacking.

# III. The Principle of Dual Criminality and the Principle of Speciality

No matter how much it may facilitate the judicial cooperation between states sidelining the principles that traditionally govern such cooperation, the abandonment of the dual criminality principle remains a choice that carries a serious risk: The service provider with a designated establishment or legal representative in the enforcing state will be obliged to contribute to the punishment of a conduct that would go unpunished in the territory of the enforcing state. This may result in imposing burdensome measures on individuals that the competent authorities of the enforcing state would not be able to take if the same conduct had occurred within their jurisdiction.

The Regulation on European Production and Preservation Orders does not really mitigate this risk. The provision of Art. 12 para. 1 (d), which, in combination with Art. 8 of the Regulation, stipulates as a ground for refusal of a European Production Order the non-criminalization of the conduct in the enforcing state, was intended to limit the aforementioned risk. However, it is accompanied by the classic exception of a list of offenses for which the dual criminality requirement is not necessary when the issuing state provides for a maximum penalty exceeding three years. Except for that, the principle of dual criminality only applies in cases where two specific categories of electronic evidence are requested: traffic data and content data. As a result, the restriction of dual criminality does not apply in cases of data requested for the sole purpose of identifying the user and subscriber data. Therefore, the aforementioned risk of producing and preserving these particular categories of data for conducts that do not constitute an offense in the enforcing state still remains more than real. Furthermore, there is no provision regarding the application of the dual criminality principle in cases of European Preservation Orders, regardless of whether they concern subscriber data, data requested for the sole purpose of identifying the user, traffic data, or content data; this is based on the thought that electronic evidence under European Preservation Orders does not result in the disclosure of the aforementioned data.[10] According to this argument, a European Preservation Order constitutes a prerequisite for the issuance of the European Production Order, which is subject to the aforementioned review of the principle of dual criminality, so the examination of the dual criminality principle will be carried out at a later stage.

The tendency to bypass the principles that traditionally govern the field of judicial cooperation in criminal matters is highlighted by the complete abandonment of the principle of speciality, which had already been set aside by the Directive regarding the European Investigation Order.[11] Thus, evidence electronically acquired through cooperation between Member States in criminal matters can apparently be used for purposes other than those for which cooperation was sought, leaving the door wide open for the evidentiary exploitation of inadvertent findings.

# IV. Remedies Available to Individuals Involved in the European Production and Preservation Orders

Legal safeguards for individuals whose data are collected, irrespective of whether they are suspects, defendants, or third parties, seem to be primarily confined to cases of European Production Orders. These legal remedies are provided by the state issuing the Order, and the individuals concerned can contest the legitimacy, necessity, and proportionality of the measures before the competent authorities of the issuing state. Therefore, electronic evidence collected under a European Preservation Order remains outside the scope of legal remedies on the grounds that it alone does not result in the disclosure of data and after all, if the issuance of the European Production Order follows, then the review can be carried out within the framework referred to in Art. 18 of the Regulation. However, it should not be overlooked that the service provider may have an obligation under its domestic legislation to delete or restrict the processing of data for which the retention was requested through the European Preservation Order. Therefore, the retention of data under the European Preservation Order that should have been deleted or where processing should at least be restricted leads to a violation of the rights of the individuals regarding the protection of their personal data and their private and family life. And all of this at a time when the retention period of the data by the service provider can be extended from the initial sixty days period by an additional thirty days (Art. 11 para. 1), and then for an indefinite period, until the European Production Order is issued or revoked, without any upper limit on the retention of such data.

Moreover, the absence of an explicit provision guaranteeing the exercise of legal remedies within the enforcing state should also be noted, which could create serious issues regarding the effectiveness of the legal protection provided, since the persons concerned would have to resort to the issuing state to exercise their rights, which is inherently challenging. However, the addition made in Art. 18 para. 2 *in finem* of the Regulation regarding the guarantees of fundamental rights in the enforcing state should not only serve as a semantic safeguard but should also be considered to 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.

# V. Conclusion

This article raised three cutting-edge issues of the new Regulation on electronic evidence in criminal matters, as they touch upon the most sensitive aspects of mutual judicial cooperation within the EU: the legal basis of the Regulation, fundamental principles of interstate cooperation, and protection of rights / effective remedies for the individuals concerned. While judicial cooperation between Member States appears to be deepening and taking new forms, it seems to be happening at the expense of rights and principles safeguarding the fundamental freedoms of individuals. The deepening of this cooperation does not serve as an end in itself but is only meaningful if it serves the freedoms of individuals. And this cannot be sidelined. In conclusion, efforts should be made to ensure that legal safeguards are in place to protect the rights of individuals subject to the European Production and Preservation Orders, including robust mechanisms for

https://doi.org/10.30709/eucrim-2023-015

contesting the legality and necessity of measures, as well as clear provisions for legal protection within the enforcing state. Such reforms would contribute to a more balanced and rights-based approach within the system established by the Regulation.

1. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.↩
2. Art. 10(2) (e) of the EIO Directive, *op. cit.* (n. 1).↩
3. Art. 30 of the EIO Directive, *op. cit.* (n. 1).↩
4. Arts. 12(3) and (4) of the EIO Directive, *op. cit.* (n. 1), where the executing authority in the European Investigation Order has a deadline of 30 days to recognize the request and must execute the order within 90 days.↩
5. See 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 harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings", SWD (2018) 118 final, table 5, p. 41.↩
6. 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, *O.J.* L 191, 28.7.2023, 118-180.↩
7. Art. 9 of the General Data Protection Regulation, *O.J.* L 119, 4.5.2016, 38.↩
8. The addressee is obliged to execute the order - meaning to transmit the data within 10 days or within 8 hours in case of emergency, see Art. 10 of the Regulation, *op. cit.* (n. 6).↩
9. Art. 15 of the Regulation, *op. cit.* (n. 6).↩
10. The Explanatory Memorandum of 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) 225 final, reads as follows at p. 22: "Given that the European Preservation Order itself does not result in data disclosure and therefore does not give rise to similar concerns, the review procedure is limited to the European Production Order".↩
11. Regarding this principle, see Arts. 27(2) and (3) of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant, *O.J.* L 190, 18.07.2002, 1.↩



ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union