European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU

Implications of the Union Legislator's Choice to Derogate from the Precedence of Union Law in the E-Evidence Regulation

Jorge A. Espina Ramos *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

The 2023 e-evidence Regulation – the new mutual recognition instrument introducing Preservation and Production Orders to obtain e-evidence from service providers – includes a provision allowing issuing authorities to decide freely whether to use this new instrument or to resort to alternative ones, even if they are not based on EU Law. This may enhance the efficiency of e-evidence gathering, but it could also have negative implications for several other issues. This article outlines the pros and cons of the legislative approach taken in the regulation of e-evidence in the EU. The author stresses that the competent issuing authority should assess all relevant factors to ensure an informed decision on the appropriate legal basis for requesting e-evidence from abroad.

AUTHOR

Jorge A. Espina Ramos

Prosecutor; Deputy National Member for Spain; Contact Point of the European Judicial Network in Criminal Matters (EJN)
Eurojust

Preprint eucrim 2025, Vol. 20(3)
https://eucrim.eu
ISSN:

The Cheshire Cat: "Then it doesn't much matter which way you go".

Alice: "… so long as I get somewhere".

Lewis Carroll (*Alice in Wonderland*)

I. Introduction

The main piece of the legislative package on electronic evidence – Regulation 2023/1543[1] (hereinafter: the e-evidence Regulation) establishes a new mutual recognition instrument for preserving and obtaining e-evidence from service providers located in another jurisdiction by means of European Preservation Orders (EPOC-PR) and European Production Orders (EPOC). It will be applicable in the EU Member States (except Denmark) as of 18 August 2026.[2]

As has often been stressed, this mutual recognition instrument, especially the revolutionary approach of allowing trans-border requests to be sent directly from the judicial authority of one Member State to the service provider of another Member State, takes the field of judicial cooperation beyond its traditional boundaries.[3] It exceeds the scope of this article to discuss the novel, revolutionary features of the e-evidence Regulation; instead I will deal with an important practical question, namely the relationship between the e-evidence Regulation and other instruments, agreements, and arrangements on the gathering of electronic evidence. In other words, the article explores how the e-evidence Regulation apparently derogates from the principle of precedence of Union law, as it does not foresee an exclusive use of EU law in judicial cooperation. As a result, the question also follows as to whether or not this is consistent with Art. 82(1) TFEU?

I will first outline the principle of the precedence of EU law under the mutual recognition instruments that were adopted prior to the e-evidence Regulation (II.). Next, I will present the provision adopted under the e-evidence Regulation (III.) before exploring several problematic issues arising from the legislative choice made by the Union legislature in the e-evidence Regulation (IV.). Section V. of the article summarises the main conclusions drawn.

II. Mutual Recognition Instruments and the Precedence of EU Law

The development of the EU's principle of mutual recognition for judicial cooperation in criminal matters began in 2002 with the Framework Decision on the European Arrest Warrant.[4] The Framework Decision was complemented by a dozen other legal instruments that regulated other scenarios of judicial cooperation in criminal matters within the EU. As an underlying principle, all these mutual recognition instruments underscored that if a legislative act of the Union exists (be it a Framework Decision, a Directive, or a Regulation) its application is considered to prevail; legal practitioners from EU Member States are theoretically not free to opt for a different instrument in their reciprocal relations, not even if other international treaties would be applicable to the subject matter. Since the beginning, however, this precedence has not been an absolute principle and we have already seen exceptions to this rule – always subject to certain conditions. For example, Art. 31(2) of the Framework Decision on the European Arrest Warrant provides that the use of alternative means is allowed:

> […] in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended or enlarged and help to simplify or facilitate further the procedures for surrender of persons who are the subject of European arrest warrants."

https://doi.org/10.30709/eucrim-2025-018

This begs the question of whether this legal assessment has changed after the entry into force of the Lisbon Treaty. Art. 82(1) TFEU states that "(j)udicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions (…)". One could argue that the wording used by the Treaty ("shall be based") does not imply an absolute obligation to govern all matters of judicial cooperation via mutual recognition and that some exceptions would be possible. Put differently, one could take the view that, although the basis for cooperation needs to be mutual recognition, this does not prevent alternative options from being acceptable. This interpretation seems to be in line with the legislative choice made in Art. 34(3) of Directive 2014/41 on the European Investigation Order (EIO Directive):

> In addition to this Directive, Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with other Member States after 22 May 2017 only insofar as these make it possible to further strengthen the aims of this Directive and contribute to simplifying or further facilitating the procedures for gathering evidence and provided that the level of safeguards set out in this Directive is respected.

Elsewhere, I have called this approach the "compatibility rule".[5] This rule has been taken up in other mutual recognition instruments, most recently in the Regulation on the transfer of proceedings in criminal matters.[6]

However, I believe that said legislative approach does not actually imply a derogation from the precedence of EU law but rather its opposite: it is only because the EU law contains this exception, that the option to use other instruments is valid. This is corroborated by the fact that the alternatives can only be used if certain conditions are met (e.g., strengthening the aims of the Directive, simplifying or facilitating the gathering of evidence, and maintaining the level of safeguards). Hence, what appears to be a derogation from the precedence of EU law is, in fact, non-existent. Only expressly authorised derogations from the principle of the exclusive application of EU law would be possible, which also has a number of implications, as we will see in a moment.

III. The e-Evidence Regulation – A New Approach

The reality under the e-evidence package is precisely that the prudent approach followed for the European Arrest Warrant, the European Investigation Order, and the Regulation on transfer of proceedings (allowing for the use of alternative legal tools only under certain conditions) has become a fully open door. In all cases, and without being subject to any conditions, any applicable different legal bases can be used instead of the Regulation, even if they are not EU legal instruments. This is due to Art. 32(1) of the e-evidence Regulation, which states:

> "This Regulation does not affect Union or other international instruments, agreements and arrangements on the gathering of evidence that falls within the scope of this Regulation."

According to this clear wording, no precedence is given to the EU Regulation and no limits or conditions are set[7] to allow for the use of alternative means. In practice, this means that competent issuing authorities remain free to decide whether they will use the EPOC/EPOC-PR or whether they will instead resort to alternative legal bases, either from the EU environment (e.g., the Directive on the European Investigation Order) or non-EU frameworks (e.g., the Council of Europe Budapest Convention on Cybercrime[8] and/or its Second Additional Protocol,[9] the UN Convention against Cybercrime (UNCAC), etc.).[10]

Sometimes, the reasons behind this legislative decision might be sound and reasonable. For instance, in complex cases in which a number of investigative measures of different nature are needed, it might be better and more efficient to allow competent authorities to use alternative legal bases, including non-EU frameworks, in addition to EU legal solutions. In this context, Recital 96 of the e-evidence Regulation clarifies:

> Member States' authorities should choose the tool most adapted to the case at hand. In some cases, they might prefer to use Union and other international instruments, agreements and arrangements when requesting a set of different types of investigative measures that are not limited to the production of electronic evidence from another Member State.

Therefore, judicial authorities can decide whether or not to use the e-evidence Regulation, even partially (e.g., use the EPOC-PR but then use a conventional mutual legal assistance (MLA) request to obtain actual evidence; or, the other way around, to use other means to preserve the data first and then use the EPOC to get the e-evidence). This approach is also reflected in other provisions of the e-evidence Regulation,[11] leaving no doubt about the intention of the Union legislator to fully confer free choice when it comes to selecting the right legal basis by which to obtain electronic evidence.

IV. Problematic Issues

Despite the reasonable grounds for this legislative approach, which allows for free choice, a number of interesting follow-up questions arise from a practical viewpoint:

Firstly, I wonder to what extent this legislative decision is in line with the wording of Art. 82(1) TFEU, which states that judicial cooperation shall be based on the mutual recognition principle. I concluded in Section II that Art. 82(1) TFEU authorises derogations from the general principle of mutual recognition, but they must also respect the clear mandate of Art. 82(1). This may mean that an issuing authority cannot be empowered to conduct intra-EU judicial cooperation based on non-mutual recognition instruments without conditions. Derogations must ensure that the choice of legal instrument is based on an assessment respecting the substantial features of mutual recognition, such as the level of safeguards or efficiency, as exemplified by the respective provisions in the Directive on the European Investigation Order and the Regulation on transfer of proceedings in criminal matters.

Secondly, the e-evidence Regulation's approach may create a disincentive for judicial authorities to use the Regulation as a legal basis for the rather simple act of data preservation, as this can be achieved more efficiently and swiftly through police channels, e.g., the services provided by the 24/7 Network established by Art. 35 of the Budapest Convention. In many countries this network fully remains under the remit of the police and not of the judiciary. When faced with the option of issuing an EPOC-PR, law enforcement might opt for the faster and more effective route of using the 24/7 Network, thus circumventing the judicial mechanisms established by the EPOC-PR.

Thirdly, the "free choice principle" might have unintended consequences for cost reimbursement. Art. 14 of the e-evidence Regulation regulates the reimbursement of costs for service providers. Specifically, paragraph 1 allows service providers to claim reimbursement of their costs from the issuing State if this is provided for under the national law of the issuing State for domestic orders in similar situations. Similar provisions do not exist in alternative legal frameworks (such as the CoE Budapest Convention and its Second Additional Protocol). Cost reimbursement may also be regulated differently, as in the EIO Directive, where the executing State bears the costs in principle. A report on cost reimbursement systems in judicial cooperation with service providers by the SIRIUS Project rightly stated:[12]

> Given the varying cost reimbursement systems across different legal frameworks (or the absence of such systems under certain frameworks), the most cost-efficient options for judicial cooperation when accessing electronic evidence might be preferred. This may involve opting for the regimes that do not include cost reimbursement provisions.

Fourthly, Art. 32(1) of the e-evidence Regulation will surely have an impact on the electronic communication channels for submitting requests. The EU has established an obligation to transmit all forms and communications related to judicial cooperation through a new digital system (originally called e-EDES,[13] recently rebranded as JUDEX[14]). The use of this digital system is mandatory by default, with only limited exceptions, and requires a completely different environment for all relevant actors, including judicial authorities. The obligation to use the system is established by the e-evidence Regulation[15] and, for other existing instruments of judicial cooperation in the EU, by Regulation 2023/2844.[16]. However, Art. 32 of the e-evidence Regulation does not prevent any competent authority from resorting to alternative means (and thus communication channels) to obtain electronic evidence. For instance, due to lack of technical resources, insufficient training, lack of knowledge, or familiarity with the new system, etc., an authority can decide that it is in the best interest of the case not to use the EU's JUDEX system by instead of using EPOC/EOPC-PR, resort to traditional means of mutual legal assistance under the Budapest Convention in order to request the evidence.[17] .

From the latter context, an interesting question further arises: whether Art. 32 of the e-evidence Regulation allows for a direct switch from EPOC/EPOC-PR to a mutual legal assistance request or whether an assessment is first required to determine if the best alternative would be to issue a European Investigation Order. If we follow the latter path, this means that resorting to mutual legal assistance requests would only be possible if the requirements of Art. 34(3) of the EIO Directive are met. Against the background that Art. 32 of the e-evidence Regulation is both *lex posterior* and *lex specialis* to the EIO Directive, a direct jump from EPOC/EPOC-PR to mutual legal assistance is possible in my opinion and would not infringe any norms stemming from either the e-evidence Regulation or the EIO Directive.

The legal situation is different, however, when it comes to the gathering of "evidence in electronic form", which is outside the material scope of the e-evidence Regulation. According to Art. 3(8), e-evidence under the e-evidence Regulation is defined as "subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form". By contrast, the Budapest Convention and its Second Protocol have a broader scope applying to "the collection of evidence in electronic form" of a criminal offence.[18] The EIO Directive, of course, also has a wider scope than the e-evidence Regulation. Consequently, if a judicial authority seeks to gather electronic evidence that is not strictly e-evidence, it must do so within the European Union through a European Investigation Order under the EIO Directive, rather than via MLA means (e.g., the Budapest Convention and its Second Protocol), unless the conditions of Art. 34(3) of the EIO Directive are met.

V. Conclusion

The 2023 e-evidence Regulation will certainly bring many novel – almost revolutionary – elements to the field of judicial cooperation. Its approach to the non-exclusive application of Union law, however, is not without problems, as this article has demonstrated. Legal practitioners need to address this approach with an open mind and even a new mind-set, when dealing with the e-evidence Regulation as it is a unique cooperation instrument for many reasons.

In this article, I have highlighted that the application of this instrument coincides with the formal revolution of digitalisation in cross-border judicial cooperation, as introduced by the JUDEX system. The e-evidence Regulation will be the first (and, for the time being, only) instrument for which the obligation to work through JUDEX applies. The EPOC-PR and EPOC as non-exclusive means to obtain e-Evidence within the EU, coupled with the implications of the Union legislator's choice to derogate from the precedence of Union law, underscores the complexity of the e-evidence landscape and sets the stage for international cooperation on digital evidence.

https://doi.org/10.30709/eucrim-2025-018

Moving forward, any judicial authority in the EU Member States should be made aware of the new possibilities at hand to gather electronic evidence. At the same time, judicial authorities must be kept informed about the potential consequences of relying on a more convenient legal basis for requests to obtain electronic evidence from other jurisdictions, as Art. 32 of the e-evidence Regulation appears to open this gateway.

1. 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, OJ L 191, 28.7.2023, 118.↩
2. For the e-evidence package, see T. Wahl, "E-evidence Regulation and Directive Published", *eucrim* 2/2023, 165-168 as well as the articles in this special *eucrim* issue on electronic evidence, pp. 170 et seq. In accordance with Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark has not taken part in the adoption of the e-evidence Regulation and is neither bound by it nor subject to its application.↩
3. Among others, see A. Juszczak and E. 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*, 182-200.↩
4. Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002, 1.↩
5. J. A. Espina Ramos, "The European Investigation Order and its Relationship with Other Judicial Cooperation Instruments", (2019) *eucrim*, 53-60, 56.↩
6. Regulation (EU) 2024/3011 of the European Parliament and of the Council of 27 November 2024 on the transfer of proceedings in criminal matters, OJ L, 2024/3011, 18.12.2024. Its Art. 33(2) reads: "In addition to this Regulation, Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with other Member States after 7 January 2025 only insofar as such agreements or arrangements make it possible to further strengthen the aims of this Regulation and contribute to simplifying or further facilitating the procedures for transferring criminal proceedings and provided that the level of safeguards set out in this Regulation is respected." It should be noted that the Regulation is applicable only as of 1 February 2027.↩
7. Such as the requirements to align with the aims of the Regulation, to have the same level of safeguards, or to strive for a higher efficiency.↩
8. Convention on Cybercrime (ETS No. 185), signed in Budapest on 23 November 2001, entered into force on 1 July 2004.↩
9. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), signed in Strasbourg on 12 May 2022.↩
10. For an overview of current national, European, and international legal efforts to regulate cross-border access to electronic evidence, see. K. Pfeffer, "Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln", (2023) *eucrim*, 170-174.↩
11. For instance, Art. 6 of the e-evidence Regulation states that an EPOC-PR can be issued "with a view to issuing a subsequent request for production of those data via mutual legal assistance, a European Investigation Order (EIO) or a European Production Order".↩
12. Cf. <https://www.eurojust.europa.eu/publication/cost-reimbursement-system>, p. 4 with further reference. SIRIUS is an EU-funded project that helps law enforcement and judicial authorities access cross-border electronic evidence in the context of criminal investigations and proceedings.↩
13. e-EDES stands for e-Evidence Digital Exchange System.↩
14. JUDEX stands for Justice Digital Exchange System. JUDEX is the reference software developed by the European Commission for connection to the Europe-wide IT system e-CODEX (e-Justice Communication via Online Data Exchange). JUDEX enables digital, secure, and fast requests for legal assistance in civil and criminal matters (e.g., European Investigation Orders) to be made to other EU Member States via the e-CODEX system.↩
15. See Arts. 19 et seq. Of Regulation 2023/1543, op. cit. (n. 1).↩
16. Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, OJ L, 2023/2844, 27.12.2023. For the use of the system in cases of transfer of proceedings in criminal matters, see Arts. 24 et seq. of Regulation 2024/3011, *op. cit.* (n. 06).↩
17. With regard to the choice between EPOC/EPOC-PR and the European Investigation Order (EIO), this would merely result in a postponement, as the use of JUDEX will also be mandatory for transmitting EIOs. However, according to current planning, this requirement will only apply from 1 March 2028, whereas the application of JUDEX for EPOC/EPOC-PR will begin earlier.↩
18. See Art. 14.2. b and c. and, similarly, Arts. 23 and 25 of the Budapest Convention (*op. cit.* (n. 8), and Art. 2.1. a of the Second Protocol to the Budapest Convention (*op. cit.* (n. 9)). According to the T-CY Guidance Note #13, "The scope of procedural powers and of international co-operation provisions of the Budapest Convention", adopted on 27 June 2023, T-CY(2023)6, available at: < https://rm.coe.int/t-cy-2023-6-guidance-note-scope-of-powers-v9adopted/1680abc76a>, p. 4, the CoE instruments do not only apply to cybercrime-related offences but to any offence, including corruption, money laundering, murder, terrorism, trafficking in human beings, etc.↩

Author statement

The opinions expressed by the author in this article are purely personal.

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