The E-evidence Package

The Happy Ending of a Long Negotiation Saga

Gianluca Forlani *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

The following article gives an overview of the long internal negotiations on the EU legal instruments aiming at improving cross-border access to e-evidence in judicial proceedings (the so-called e-evidence package), which have finally been concluded. It outlines the main challenges met during the negotiations and how they were overcome to reach a compromise which has become subject to political agreement. This compromise is expected to prove more useful from a practical point of view than previous, more general cooperation tools. In addition, the article puts the EU's legislative initiative into the context of legal instruments and negotiations on law enforcement access to e-evidence at the international level before turning to expected future developments.

AUTHOR

Gianluca Forlani

Judge

CITE THIS ARTICLE

Forlani, G. (2023). The E-evidence Package : The Happy Ending of a Long Negotiation Saga. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-013

Published in eucrim 2023, Vol. 18(2) pp 174 – 181

https://eucrim.eu

ISSN:

I. Introduction

Legislative initiatives on e-evidence were presented more than five years ago. After conducting an in-depth assessment and following bilateral discussions with the delegations of the EU Member States, the European Commission published two proposals on 17 April 2018:

- A proposal for a Regulation on the European orders for the production and preservation of electronic evidence in criminal matters;[1]
- A proposal for a Directive establishing harmonised rules on the appointment of legal representatives for the purpose of obtaining evidence in criminal proceedings[2].[3]

These instruments and the ensuing negotiations faced several complex challenges. One of the main challenges was striking a fair balance between the fundamental rights related to the protection of privacy and the rights of suspects and accused persons on the one hand, and enabling/facilitating investigations and prosecutions of crime on the other.

While even with traditional judicial cooperation instruments, this balance is always difficult to strike, the specific case of e-evidence encountered a further obstacle: the need for a direct relationship between the judicial authority of a prosecuting state (issuing state) and a (private) entity outside its jurisdiction, i.e. a service provider who holds data that may include traces of communications and activities of perpetrators who operate through IT means. Thus, this "e-evidence scenario" deviates from the traditional trilateral relationship on the basis of mechanisms of letters rogatory that require the involvement of the judicial authority of the state where the service provider is located. This resulted in the fundamental question to which extent the judicial authority in the service provider state was to actively be involved . Should the latter simply be obliged to execute the order of the issuing judicial authority? Should it verify the correctness of the activity carried out by the issuing authority? In short, the e-evidence package was a real litmus test for the principles of mutual trust and mutual recognition that kept being invoked and flaunted throughout the negotiations. This raised the more general question of whether "mutual trust" means "blind faith" or "reasoned trust".

The following section (II.) outlines the background of the internal EU legislative rules on e-evidence and critical issues that emerged during the negotiations; this culminated in the provisional agreement of 25 January 2023 and – after linguistic and technical revision – the final texts that were signed on 12 July 2023 and published in the Official Journal of the European Union on 28 July 2023.[4] However, the EU's e-evidence package must also be seen in the context of the overall legal framework on e-evidence at the international level (comprised of the Council of Europe Second Additional Protocol to the Cybercrime Convention, the bilateral negotiations on an EU-US e-evidence agreement, and the starting negotiations on a United Nations legal instrument on cybercrime), to which Section III. is dedicated. Section IV. of this article provides a brief outlook to the next steps of the EU dossier before additional and concluding remarks (Section V.).

https://doi.org/10.30709/eucrim-2023-013

II. Background and Negotiations of the EU Legal E-evidence Package

1. Challenges/issues of electronic evidence acquisition in the current legal framework

Prior to the new e-evidence package, multiple international cooperation instruments had been used under the EU legal framework for cross-border electronic evidence gathering. These instruments include:

- Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO)[5];
- The European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;[6]
- Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust);[7]
- Regulation (EU) 2016/794 on Europol;[8]
- Council Framework Decision 2002/465/JHA on joint investigation teams;[9]
- Bilateral agreements between the Union and third states, such as the mutual legal assistance agreements in force with the US;[10]
- The Council of Europe Convention on Cybercrime (Budapest Convention).[11]

Yet in practice, these comprehensive and wide-ranging legal cooperation instruments have still failed to adequately address some of the difficulties encountered in the process of obtaining electronic data. One of the most significant obstacles in this context has been the refusal by Internet service providers to make data available in cases where the authority in question lacks jurisdiction over the place of the establishment of its headquarters, or because of the nationality of the affected person for whom data has been requested. More complex problems arise when a case is connected with the legal system of states outside the EU (third states), which is a recurring scenario given that the largest providers of telematic services are based in the United States.[12] In addition to the aforementioned jurisdictional problems, obtaining electronic evidence through judicial cooperation procedures – whether conventional or based on the principle of mutual recognition – has always necessitated the involvement of the (judicial and/or governmental) authority of the executing/requested state. This inevitably causes delays, which is clearly incompatible with the "volatility" of electronic data.

2. The Commission's two regulatory proposals

With the two proposals listed earlier,[13] the Commission intended to overcome these shortcomings. Notwithstanding this ambition, they are designed to complement, and not replace, existing judicial cooperation instruments, in particular the EIO. The Regulation aims to simplify and accelerate the process of securing and obtaining electronic evidence stored and/or held by service providers established in another jurisdiction. This objective is to be achieved by directly transmitting the order to preserve/produce data to the representative designated by the service provider, with the latter being obliged to comply by directly handing over the data to the requesting authority. This obligation applies unless there are specific and compelling reasons not to do so, and without being able to oppose reasons related to the place where the data are stored. In turn, the

corresponding Directive aims to establish an obligation for service providers offering their services in the EU to designate a legal representative in at least one Member State.

It follows that the relevant procedural mechanisms need to be structured according to general models to make them useful from an operational point of view and ultimately ensure their practical applicability. In other words, the negotiations made it clear that unless speed and efficiency are to be improved with a new European production order, the prosecuting authorities would continue to use the cooperation tools already available.

3. Critical pre-trilogue issues emerged in the Council

Negotiations on the two proposals started in the COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency, and continued under the subsequent Council presidencies. From the outset, the process placed great emphasis on working around the principle of territoriality in the traditional sense, which was achieved by declaring the location of the data to be irrelevant. However, some technical issues immediately emerged as harbingers of several other critical points. These included:

- Potential conflicts with obligations under the law of third countries (and, in this context, the relationship between the proposed new instrument and the US CLOUD Act);
- A possible extension of the subject matter of the Regulation to include direct access to data by authorities and real-time interceptions, which are considered to be extremely relevant investigative tools;
- The question of whether orders should also be served to the relevant authority of the executing state or of another state that has a connection with the case at issue.

The Austrian Council presidency presented a compromise text (which reflected the negotiating efforts of the Member States to reach an agreement) to the Justice and Home Affairs (JHA) Council in December 2018.[14] At this meeting, the Council's general approach on the draft Regulation was adopted while that on the draft Directive was reached in the JHA Council in March 2019. While the Member States supported the compromise text of the Austrian presidency, some called for subtle changes. For example, two states suggested introducing a more incisive procedure of notifying authorities in the affected persons' states; others would have preferred a more streamlined procedure that would have seen no other authorities or states notified at all.

4. Pre-trilogue contributions by other institutions

The European Economic and Social Committee adopted its opinion as early as on 12 July 2018. Conversely, the European Parliament (EP) as co-legislator appointed its rapporteur on 24 May 2018. Subsequently, several meetings and hearings were held in the LIBE Committee on the e-evidence proposal, including a public hearing on 27 November 2018.

The LIBE Committee developed amendments to numerous key provisions of the regulation, being in strong contrast with the Council's general approach. The Committee, *inter alia*, proposed replacing the Directive and integrating some of its provisions into the Regulation (a solution that casted serious doubts on the appropriateness of the latter's legal basis). The large number of proposed amendments tabled by the parliamentary political groups, together with the onset of the pandemic, further slowed down work on a final EP position, which was finally adopted as late as in mid-December 2020.[15] The EP's text was still far from the one that

the Council had drafted in its general approach. The EP followed a much more restrictive approach on central issues, such as:

- The prerequisites for issuing orders (three additional prerequisites were inserted);
- The need for notification to the executing state with substantial effects for all orders and for all types of data;
- The extension of the grounds for refusal and the inclusion of mandatory ones;
- The merger of the Directive with the Regulation.

A rather carefully-worded position was also expressed by the European Data Protection Supervisor (EDPS) on 6 November 2019.[16] On the one hand, the EDPS supported in his opinion "the objective of ensuring that effective tools are available to law enforcement authorities to investigate and prosecute criminal offences, and in particular welcomed "the objective of the Proposals to accelerate and facilitate access to data in cross-border cases by streamlining procedures within the EU." On the other hand, the EDPS underlined "that any initiative in this field must be fully respectful of the Charter of Fundamental Rights of the EU and the EU data protection framework…" The EDPS advocated for a greater involvement of judicial authorities in the enforcing Member States and expressed a wish for them to be "systematically involved as early as possible in this process" in order to "have the possibility to review compliance of orders with the Charter and have the obligation to raise grounds for refusal on that basis." In addition, the EDPS voiced the need to clarify the definitions of data categories in order to make them consistent with other definitions of data categories in EU law. He eventually recommended "reassessing the balance between the types of offences for which European Production Orders could be issued and the categories of data concerned in view of the relevant case law of the Court of Justice of the EU."

5. The trilogue negotiations and compromise

The inter-institutional negotiations between the Commission, the Council, and the European Parliament (the so-called trilogue) started in January 2021 under the Portuguese Council presidency. The trilogue negotiations spanned four further Council presidencies (Slovenia, France, the Czech Republic, and Sweden). At the beginning of 2023, a compromise was found under the Swedish presidency.

Trilogue turned out to be particularly complex due to the profound differences between the text of the Council's general approach and the EP's position. The EP advocated a much more restrictive instrument, having proposed to introduce a greater number of prerequisites for orders by the issuing authority and a generalised regime of notification to the state of execution covering all orders and all types of data with substantial effects. This was accompanied by an extensive list of grounds for refusal, some of which were considered mandatory. Moreover, the EP proposed abandoning the Directive, incorporating some of its provisions into the Regulation (cf. above 4.).

On the part of the Council, diverging views emerged: Some more ambitious delegations supported the solution proposed in the general approach, considering it suitable to guaranteeing an adequate level of effectiveness of the instrument and at the same time high standards of protection of fundamental rights; yet other delegations reiterated their general support for a stronger and more extensive notification regime, while considering some options of the EP to be overly restrictive. In the absence of any obvious willingness to compromise on the part of the EP's negotiators, the Council conducted the negotiations by sticking as closely as possible to the text of the general approach during this initial phase.

https://doi.org/10.30709/eucrim-2023-013

Given the EP's persistence on its position, the Council adopted a different approach in the second half of 2021 and suggested compromise solutions, showing some flexibility with respect to its general approach. Such solutions included, for instance, the suggestion that all forms of notification for preservation and production orders related to subscribers' data and so-called identification data (traffic data used solely for identification purposes, such as IP addresses, ports, etc.) be removed. In addition, no notification was to be needed for production orders of traffic data belonging to subjects residing in the issuing state, whereby such residence was to be presumed unless there were reasonable grounds to believe otherwise.

Even though this compromise solution was supported by the Member States (primarily as *ultima ratio* in order to break the deadlock), the EP found it insufficient in view of fundamental rights concerns.

Nevertheless, the Council continued its efforts to reach a final agreement on the instruments by tabling new compromise texts. In particular, issues not related to notification (on which a preliminary agreement had not yet been reached between the co-legislators) were brought back to the negotiating table. The discussion on the proposal for a Directive on harmonised rules for the appointment of legal representatives for the purpose of obtaining evidence in criminal proceedings, previously shelved as particularly controversial, was reopened. The debate on the Directive was fruitful, with the EP accepting to maintain the Directive as a separate instrument and as a way of settling good compromise solutions on almost all outstanding issues.

At the same time, the Council drew up a compromise proposal. While still aiming to uphold the residence criterion for both content and traffic data, it included some key points of the EP position, such as a single regime for content and traffic data, notification with suspensive effect, and a list of grounds for non-execution, including at least immunities and privileges, fundamental interests and security of the executing state, freedom of the press and freedom of expression, and fundamental rights. The proposal was supported by the majority of Member States, but attempts to reach an agreement with the EP were unsuccessful.

Following a deadlock, the dialogue between the EP and the Council resumed in May 2022. Despite significant disagreement on crucial issues (notification, grounds for refusal, residence criterion), intense negotiating efforts by the parties allowed them to make good progress in bilateral discussions. At the end of 2022, attempts were intensified to finally reach an agreement, in line with the Commission's position. At the meeting of the Permanent Representatives Committee on 23 November 2022, the Council presidency asked the Member States to be granted a mandate for the trilogue meeting on 29 November to present an overall compromise package. This package, which was finally agreed on by both the Member State delegations and the EP, included the following:

- Application of the residence criterion to exclude notification to the executing state: Due to the burden of proof of residence being reversed and put on the issuing authority, the EP insisted on setting a number of requirements for proof of residence (e.g. proof by way of an identity document or entry in a public register, a minimum period of residence, and other circumstances that were considered to be mandatory). In practice, this makes such proof very difficult for the issuing authority. It was, however, agreed that said requirements were to be placed in a recital, with the understanding that they would be mere indicators that could be used to prove the stability of permanence in the territory of the issuing state, rather than representing necessary and prescriptive requirements.[17]

- Refusal of orders as a consequence of a pending rule-of-law procedure under Art. 7(1) and (2) of the Treaty on European Union (TEU): The EP initially proposed inserting grounds for refusal that referred to a pending Article 7 TEU procedure against the issuing State dealing with serious violations of the values mentioned in Article 2 TEU into the operative part of the Regulation. This was moved to a recital[18]and rephrased to avoid any automatism.

https://doi.org/10.30709/eucrim-2023-013

- Optional nature of the grounds for refusal and limited role of the service provider in non-execution of orders: The final compromise[19] provides that service providers may only put forward a limited number of refusal grounds. In addition, they are obliged to inform the issuing authority and, if notification is required, the enforcing authority before a possible non-execution. Since service providers are private entities, they are not entitled to refuse requests on the grounds of fundamental rights violations; such assessment is reserved to the discretionary power of the judicial authority of the service providers' location.

- The distinction between the service provider and the data controller: Where the data controller differs from the Internet service provider, the issuing authority has the general obligation to address the order to the controller; however, the issuing authority is granted extensive exceptions in order to not hamper or slow down the investigation.[20]

- Deletion of data: The compromise includes an obligation to delete (or alternatively restrict the use of) data transmitted in response to orders issued in urgent cases in the absence of notification if grounds for refusal emerge after transmission. This was done in respect to the EP's initial demand that the issuing authority be obliged to delete data received in an emergency case as and when grounds for refusal are raised.[21]

III. E-evidence for Criminal Proceedings: the International Context

The important step forward achieved with the EU's internal rules on access to e-evidence by the EU's judicial authorities also needs to be assessed against the background of parallel international legal instruments (existing and planned). The EU legal framework is a central starting point for negotiations on the same topic undertaken by the EU with third countries. At the same time, the new EU system constitutes an essential benchmark for verifying the consistency of other systems with the fundamental rights touched by the search and acquisition of electronic evidence, bearing in mind that it is subject to the case law of the Court of Justice of the European Union (CJEU) and, more broadly, of the European Court of Human Rights (ECtHR).

During the JHA Council meeting held on 6–7 June 2019, the justice ministers of the EU Member States approved the *Council Decision authorizing the European Commission to initiate negotiations with the United States regarding cross-border access to electronic evidence in the context of judicial cooperation in criminal matters* and the addendum containing the relevant negotiating directives.[22] However, this dialogue with the US has been suspended pending the prior conclusion of the EU internal rules. It is now about to be resumed as the EU e-evidence package has been agreed.

At the JHA Council meeting of June 2019, the ministers had also adopted the *Decision authorising the participation of the European Union in the negotiations for the adoption of a Second Protocol additional to the Budapest Convention on Cybercrime*, which handed the European Commission a mandate to represent the European Union at the Council of Europe (CoE) level.[23] The Second Protocol was finalised in December 2021, and opened for signature on 12 May 2022 under the Italian presidency of the CoE. It will enter into force after ratification by at least five states. After consent by the EP on 17 January 2023, the Council adopted a decision on 14 February 2023 authorising the EU Member States to ratify the Second Protocol, in the interest of the EU.[24] The Second Protocol provides tools to strengthen cooperation and dissemination of electronic evidence and includes the following main features:[25]

- In principle, direct cooperation between competent authorities of CoE member states and service providers of another state party;

- Effective means of obtaining subscriber information and traffic data;
- Obligation to create specific channels for rapid and direct cooperation between state authorities and between these authorities and private entities established in the territory of another state party;
- Competent state authorities may request the information necessary to identify or contact the registrant of a domain name in possession or under the control of the provider from service providers established in the territory of another state party;[26]
- Considering that the range of participants in the Budapest Convention is broader and less homogeneous than EU Member States, a state party can always claim the right to notification to filter out requests;[27]
- State authorities may require a service provider established in the territory of another state party to disclose the information on a subscriber, in possession or control of the service provider, where the information is necessary for specific criminal investigations and proceedings; [28]
- Detailed regulation of the content of the request and the time limit within which the order must be enforced. If a service provider does not disclose the requested information by the deadline or expressly refuses to provide it, the authorities of the requesting state may seek to enforce the order in accordance with the procedure set out in Art. 8;
- According to Art. 8, cooperation does not take place between the authority and the private service provider, but between the national authorities of the states concerned (requesting and requested): the requested state must make every reasonable effort to compel the service provider in its territory to disclose the subscriber information and traffic data as quickly as possible or, in any case, within the time limits laid down in the Budapest Convention;
- Establishment of a cooperation scheme in emergency cases to obtain data stored by a service provider, including accelerated communication channels;[29]
- Possibility for two or more State parties to allow their competent authorities, on the basis of mutual agreements, to establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings (where enhanced coordination is deemed to be of particular utility);[30]
- Clarification that other bilateral or multilateral agreements regulating the exchange of e-evidence are applicable, including the EU e-evidence Regulation (and the corresponding Directive) as well as any future agreements between the EU and the US.[31]

Efforts to regulate e-evidence are also ongoing at the United Nations level. Through its Resolution 74/247 adopted on 27 December 2019, *Countering the use of information and communications technologies for criminal purposes*, the UN General Assembly established an Intergovernmental Committee of Experts (Ad Hoc Committee) with representatives from all UN countries to draft a global Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The first negotiating session of the Committee took place in New York from 28 February to 11 March 2022. The General Assembly decided, *inter alia*, that the Ad Hoc Committee should convene at least six sessions of ten days each, followed by a concluding session in New York. The sixth session took place in New York from 21 August to 1 September 2023 and a concluding session is scheduled to take place in New York between 29 January and 9 February 2024. The EU also participates in the negotiation as an observer. Even though it is premature to predict the final outcome, the EU Member States' approach should be not to exceed the scope of the Second Protocol to the CoE Budapest Convention.

IV. Towards Adoption of the EU Legal Instruments – Next Steps

The e-evidence Regulation entered into force on 18 August 2023 and it will apply from 18 August 2026 (Art. 34 of the Regulation). According to Art. 33 of the Regulation, the Commission shall carry out an evaluation of it by 18 August 2029 (six years from the entry into force of the Regulation). The Commission shall transmit an evaluation report to the European Parliament, the Council, the European Data Protection Supervisor, and the European Union Agency for Fundamental Rights. This evaluation report should include an assessment of the application of the Regulation and of the results that have been achieved with regard to its objectives, and an assessment of the Regulation's impact on fundamental rights. The evaluation should be conducted in accordance with the Commission's better regulation guidelines.

As far as the Directive is concerned, Art. 7 provides that Member States must bring into force the laws, regulations and administrative provisions necessary to comply with it by 18 February 2025. The discrepancy between the date when the Regulation will become applicable in the Member States and the date to bring into force the laws, regulations, and administrative provisions necessary to comply with the Directive is obviously linked to the fact that the Directive is a necessary precondition to the Regulation. Art. 8 of the Directive provides for the Commission to carry out its evaluation by 18 August 2029, i.e., in parallel with the one of the Regulation.

V. Additional Remarks and Conclusion

Considering the relevance of electronic data as evidence, the agreement on the e-evidence package represents the achievement of a crucial tool in view of future developments in judicial cooperation in criminal matters. The most noticeable innovations of the e-evidence package concern, on the one hand, the irrelevance of the location of the data, and, on the other hand, the attempt to provide for a direct relationship between the requesting state and the service provider, with the competent authority of the executing state intervening only when the provider does not comply within a set period of time.

Given the potentially high invasiveness of the measures in question, it is noteworthy that the EU e-evidence Regulation[32] contains a number of robust procedural safeguards, for example:

- Protecting personal data by referring to the applicability of the EU General Data Protection Regulation (GDPR)[33] and the EU Data Protection Directive for police and justice activities[34];
- Providing grounds for refusal which the judicial authority of the state in which the service provider is located and who must be notified of the request for data may oppose to the requesting state, particularly to ensure the protection of fundamental rights;
- Distinguishing between the different types of data according to their intrusiveness and providing different guaranties with reference to the issuing authority: If subscriber data or data requested for the sole purpose of identifying a person (e.g., the owner of an e-mail address) are to be obtained, the order has to be issued by a judge or by a public prosecutor. If the data is considered more invasive (i.e., traffic or content data), a request by a judge is required;[35]
- Requiring that production orders may be issued in criminal proceedings in which offences are prosecuted for which a minimum term of imprisonment of four months is prescribed for the aforementioned first type of data or three years for traffic or content data. In the latter case, the possibility of issuing the order in relation to a number of particularly serious offences (albeit with a lower sanction) is also

https://doi.org/10.30709/eucrim-2023-013

provided for (i.e., fraud and counterfeiting of non-cash means of payment; sexual abuse and sexual exploitation of children and child pornography; attacks against information systems [all if they are wholly or partly committed by means of an information system] and terrorism offences);

- Providing time limits for the preservation of data until a subsequent request for production.[36]

It should finally be stressed, however, that the legal e-evidence instruments presented above regulate the access and/or the acquisition of data as evidence, which means that they presuppose the existence of such data. They do not regulate obligations to retain data. The retention of data is equally important and is closely linked to the subject matter of e-evidence. Adequate regulation on data retention cannot be negated. Even "ordinary" criminal proceedings are notoriously time-consuming, not least to ensure that a fair trial and the rights of the suspects/accused persons are duly guaranteed. Moreover, a crime is often discovered only after a considerable period of time has elapsed since the commission of the offence. If data are not retained or are retained for a too short period in such cases, all the rules governing their acquisition risk finding limited application; they might even risk remaining a purely stylistic exercise. This implies the need for striking a good balance between the strictness of the rules governing access to data and the retention of data for an adequate period of time. The CJEU has reaffirmed its stance on data retention in various judgments and emphasised that interference entailed by the retention of traffic and location data is justified only to combat serious crime or to prevent serious threats to public security.[37] It remains to be seen whether a very recent judgment (CJEU judgment of 7 September 2023 in *Lietuvos Respublikos generalinė prokuratūra*)[38] will provide fresh impetus to the discussion on the limits to and concrete rules on data retention. After a first reading of the judgment, the CJEU provided not only interesting pointers to how the leeway to regulate data retention can be implemented in the various legal systems, but also provided guidance as to the relationship between different kinds of proceedings and the mutual use of retained data. This raises the interesting question of whether a dividing line should be drawn *a priori* between the different kinds of proceedings (administrative, criminal) with a prejudicial distinction of the value of the interests protected therein or whether the level of the interests at stake should be assessed from time to time with a view to enabling the use of retained data in other proceedings regardless of their nature. At the same time, the CJEU ruled on the procedural consequences if the conditions of the Union law on data retention are not met. Whereas previous case-law left this question open, the Court now expressly precludes the use of the data as evidence.

---

1. COM(2018) 225 final.↩
2. COM(2018) 226 final.↩
3. For a summary of the proposal, see also T. Wahl, "Commission Proposes Legislative Framework for E-evidence", (2018) *eucrim*, 35.↩
4. 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; 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, *O.J.* L 191, 28.7.2023, 181–190.↩
5. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1; see also, inter alia, J.A. Espina Ramos, "The European Investigation Order and its Relationship with Other Judicial Cooperation Instruments", (2019) *eucrim*, 53.↩
6. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *O.J.* C 197, 12.7.2000,pp. 1 et seq.↩
7. Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, *O.J.* L 295, 21.11.2018, 138.↩
8. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *O.J.* L 135, 24.5.2016, 53.↩
9. Council Framework Decision of 13 June 2002 on joint investigation teams, *O. J.* L 162, 20.06.2002,1.↩
10. Agreement on mutual legal assistance between the European Union and the United States of America, *O.J.* L 181, 19.7.2003, 34.↩
11. European Treaty Series No. 185.↩
12. In this regard, it should be pointed out that the new US legislation on matters of e-evidence, i.e., the CLOUD Act approved on 23 March 2018, obliges US service providers to comply with requests for data production (even if stored outside US territory and thus, hypothetically, also on EU

territory) *only if they originate from US authorities*. By contrast, enforceable agreements between the respective foreign governments are required if data are to be delivered (even directly) to foreign authorities.↩

13. *Op. cit.* (n. 1 and 2).↩
14. Council of the EU, Press release of 7 December 2018: "Regulation on cross border access to e-evidence : Council agrees its position" <https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/> accessed 20.09.2023.↩
15. European Parliament Report - A9-0256/2020, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html>; for an interesting insight into the EP's position, see also E-Evidence Package - The Position of the European Parliament, Update 9/08/2021, <https://www.eurojust.europa.eu/sites/default/files/assets/e-evidence-package-the-position-of-the-european-parliament.pdf> accessed 20.09.2023.↩
16. Opinion 7/2019, available at: <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf> accessed 20.09.2023.↩
17. The final compromise is reflected in Recitals 52 and 53 of the Regulation, *op. cit.* (n. 4).↩
18. Recital no 64 of the Regulation: "It should be possible for the enforcing authority to refuse an order, in exceptional situations, where there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the European Production Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter. In particular, when assessing that ground for refusal, where the enforcing authority has at its disposal evidence or material such as that set out in a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission, adopted pursuant to Article 7(1) TEU, indicating that there is a clear risk, if the order were executed, of a serious breach of the fundamental right to an effective remedy and to a fair trial under Article 47 of the Charter, on account of systemic or generalised deficiencies concerning the independence of the issuing State's judiciary, the enforcing authority should determine specifically and precisely whether, having regard to the personal situation of the person concerned, as well as to the nature of the offence for which the criminal proceedings are conducted, and the factual context that forms the basis of the order, and in the light of the information provided by the issuing authority, there are substantial grounds for believing that there is a risk of a breach of a person's right to a fair trial."↩
19. Reflected in Recitals 56 to 59 and Arts. 10(2), 10(3) and 10(5) of the Regulation, *op. cit.* (n. 4). The relevant part of Art.10 reads as follows:
Execution of an EPOC
…
2. Where a notification to the enforcing authority is required pursuant to Article 8 and that authority has not raised any ground for refusal in accordance with Article 12 within 10 days following receipt of the EPOC, the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities, as indicated in the EPOC, at the end of that 10-day period. Where the enforcing authority already before the end of that 10-day period confirms to the issuing authority and the addressee that it will not raise any ground for refusal, the addressee shall act as soon as possible upon such confirmation and at the latest at the end of that 10-day period.
3. Where a notification to the enforcing authority is not required pursuant to Article 8, upon receipt of an EPOC, the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities, as indicated in the EPOC, at the latest within 10 days following receipt of the EPOC.
…
5. Where the addressee considers, based solely on the information contained in the EPOC, that the execution of the EPOC could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State, the addressee shall inform the issuing authority and the enforcing authority using the form set out in Annex III.↩
20. The final compromise is reflected in Arts. 5(6) and 5(7) of the Regulation. The relevant part of Art. 5 reads as follows: **Conditions for issuing a European Production Order**
….
6. A European Production Order shall be addressed to the service provider acting as controller in accordance with Regulation (EU) 2016/679.
By way of exception, the European Production Order may be directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, where:
(a) the controller cannot be identified despite reasonable efforts on the part of the issuing authority; or
(b) addressing the controller might be detrimental to the investigation.
7. In accordance with Regulation (EU) 2016/679, the processor that stores or otherwise processes the data on behalf of the controller shall inform the controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. In that case, the issuing authority shall indicate in the case file the reasons for the delay in informing the controller. A short justification shall also be added in the EPOC.↩
21. The final compromise is reflected in Arts. 4(5) and 10(4) of the Regulation. The relevant parts read as follows:
Article 4
Issuing authority
…
5. In a validly established emergency case, as defined in Article 3, point (18), the competent authorities referred to in paragraph 1, point (b), and in paragraph 3, point (b), of this Article may exceptionally issue a European Production Order for subscriber data or for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or a European Preservation Order, without prior validation of the order concerned, where validation cannot be obtained in time and where those authorities could issue an order in a similar domestic case without prior validation. The issuing authority shall seek *ex post* validation of the order concerned without undue delay, at the latest within 48 hours. Where such *ex post* validation of the order concerned is not granted, the issuing authority shall withdraw the order immediately and shall delete or otherwise restrict the use of any data that were obtained.
Article 10
Execution of an EPOC
4. In emergency cases, the addressee shall transmit the requested data without undue delay, at the latest within eight hours following receipt of the EPOC. Where a notification to the enforcing authority is required pursuant to Article 8, the enforcing authority may, if it decides to raise a ground for refusal in accordance with Article 12(1), without delay and at the latest within 96 hours following receipt of the notification, notify the

issuing authority and the addressee that it objects to the use of the data or that the data may only be used under conditions which it shall specify. Where a ground for refusal is raised by the enforcing authority, if the data have already been transmitted by the addressee to the issuing authority, the issuing authority shall delete or otherwise restrict the use of the data or, in the event that the enforcing authority has specified conditions, the issuing authority shall comply with those conditions when using the data.↩

22. See T. Wahl, "E-Evidence: Commission obtains Mandates for EU-US agreement and Negotiations in Council of Europe" (2019) *eucrim*, 113.↩
23. Ibid.↩
24. Council of the EU, Press release of 14 February 2023: "Access to e-evidence: Council authorises member states to ratify international agreement", <https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/> accessed 20 September 2023.↩
25. Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.V.2022, CETS No. 224.↩
26. Art. 6 of the Second Protocol.↩
27. Cf. Art. 7 para. 5 of the Second Protocol: "A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, notify the Secretary General of the Council of Europe that, when an order is issued under paragraph 1 to a service provider in its territory, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding."↩
28. Art. 7 and 8 of the Second Protocol.↩
29. Arts. 9 and 10 of the Second Protocol.↩
30. Art. 12 of the Second Protocol.↩
31. Art. 15 of the Second Protocol.↩
32. *Op. cit.* (n. 4).↩
33. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, 4.5.2016, 1.↩
34. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* L 119, 4.5.2016, 89.↩
35. Art. 4(1) and 4(2) of the Regulation.↩
36. Art. 11(1) of the Regulation.↩
37. *Inter alia*: judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland/Seitlinger et al.*); judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB/Watson et al.*); judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and Others*); judgment of 5 April 2022).↩
38. Case C-162/22.↩

Author statement

The views expressed in this article are solely those of the author and are not an expression of the views of the institution he is affiliated with.

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