# ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS AS A NEW CHALLENGE FOR EUROPEAN JUDICIAL COOPERATION*

LIBOR KLIMEK

**Abstract:** **Electronic Evidence in Criminal Proceedings as a New Challenge for European Judicial Co-Operation**

The increasing digitalisation of contemporary society has fundamentally transformed the nature of criminal investigations and the acquisition of evidence. Electronic data has become an essential source of information in criminal proceedings, while its cross-border character has exposed significant limitations of traditional mechanisms of judicial cooperation in criminal matters. In response to these challenges, the European Union adopted a new legal framework, commonly referred to as the e-Evidence package, centred upon Regulation (EU) 2023/1543 and Directive (EU) 2023/1544. This article examines the legal and constitutional implications of the e-Evidence system from the perspective of European Union law. Particular attention is devoted to the impact of the new framework on the principle of member state sovereignty within the Area of Freedom, Security, and Justice. The article seeks to answer the following research question: To what extent does the e-Evidence system affect the principle of member state sovereignty within the framework of judicial cooperation in criminal matters in the European Union? The analysis is based primarily on the doctrinal method, supplemented by analytical and comparative approaches. The article examines the concept and significance of electronic evidence, traditional mechanisms for obtaining electronic evidence in cross-border cases, the legal framework of e-Evidence, the protection of fundamental rights, and the relationship between e-Evidence and existing European structures of judicial cooperation. The article concludes that the e-Evidence system does not eliminate member state sovereignty but contributes to its transformation within an increasingly integrated European legal order.

**Keywords:** electronic evidence; e-Evidence; judicial cooperation in criminal matters; European Union; member state sovereignty; cross-border criminal proceedings

**DOI:** 10.14712/23366478.2026.118

* The contribution was elaborated as a part of the research project VEGA No. 1/0248/26 “Perspectives on Enhancing Judicial Co-operation in Criminal Matters through Transnational Units”.

© 2026 The Author. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

## INTRODUCTION

The digital transformation of contemporary society has fundamentally altered the nature of human communication, economic activity, and social interaction. An increasing proportion of information relevant to criminal investigations is no longer stored in *physical form* but exists as *electronic data* held by private service providers operating across multiple jurisdictions. E-mails, cloud storage records, subscriber information, traffic data, and communications exchanged through social networking platforms have become indispensable sources of evidence in criminal proceedings.[1] As criminal activities increasingly transcend national borders and exploit digital technologies, law enforcement and judicial authorities face growing difficulties in obtaining *electronic evidence* efficiently and lawfully. The traditional legal instruments developed for a predominantly territorial conception of criminal justice have proven insufficient to address the speed, complexity, and transnational character of *digital evidence*. Consequently, the European Union has sought to develop new legal mechanisms capable of responding to these challenges while preserving the fundamental values upon which judicial cooperation in criminal matters is based.[2]

For several decades, judicial cooperation in criminal matters within Europe was predominantly structured around the principles of state sovereignty, territorial jurisdiction, and mutual legal assistance. Under this model, authorities of one state were generally required to address requests for evidence through the competent authorities of another state, thereby respecting the latter's sovereign prerogatives over persons, activities, and data located within its territory.[3] Although the principle of mutual recognition subsequently accelerated cooperation within the *Area of Freedom, Security, and Justice*,[4] the acquisition of electronic evidence continued to encounter significant practical obstacles. Digital information is frequently dispersed across multiple jurisdictions, controlled by multinational service providers, and subject to rapidly changing technological conditions. Delays associated with traditional cooperation mechanisms have therefore increasingly been perceived as incompatible with the operational requirements

---

1 SIRIUS: Cross-Border Access to Electronic Evidence. In: *Eurojust* [online]. [cit. 2026-05-20]. Available at: https://www.eurojust.europa.eu/sirius.

2 See, for example: E-evidence – Cross-Border Access to Electronic Evidence. In: *European Commission* [online]. [cit. 2026-05-20]. Available at: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en; see also: Electronic Evidence. In: *Eurojust* [online]. [cit. 2026-05-20]. Available at: https://www.eurojust.europa.eu/judicial-cooperation/instruments/electronic-evidence.

3 AMBOS, K. *European Criminal Law*. Cambridge: Cambridge University Press, 2018, pp. 415–453; BÖSE, M. (ed.). *Europäisches Strafrecht*. 2. Aufl. Baden-Baden: Nomos, 2021, pp. 18–20; SATZGER, H. *Internationales und Europäisches Strafrecht*. 11. Aufl. Baden-Baden: Nomos, 2025, pp. 181–220.

4 JANSSENS, CH. *The Principle of Mutual Recognition in EU Law*. Oxford: Oxford University Press, 2013, pp. 166–233; KLIMEK, L. *Mutual Recognition of Judicial Decisions in European Criminal Law*. Cham: Springer, 2017, pp. 3–40; AMBOS, *c. d.*, pp. 415–453; MITSILEGAS, V. *EU Criminal Law After Lisbon: Rights, Trust and the Transformation of Justice in Europe*. Oxford, Portland: Hart Publishing, 2018, pp. 151–186; SATZGER, *c. d.*, pp. 181–220.

of effective criminal investigations, particularly in cases involving organised crime, cybercrime, terrorism, and other serious forms of cross-border criminality.

Against this background, the European Union adopted a new legislative framework commonly referred to as the e-Evidence package.[5] The introduction of the *European Production Order* and the *European Preservation Order* represent a significant development in the evolution of judicial cooperation in criminal matters. Unlike traditional mechanisms, the new framework enables competent authorities of one member state of the EU, under prescribed conditions, to address legally binding orders directly to service providers established or represented in another member state. On the one hand, this approach reflects a broader tendency within European integration towards the establishment of more direct, efficient, and technologically adapted forms of cooperation. At the same time, however, it raises complex constitutional and legal questions concerning the relationship between effectiveness of criminal justice and the continuing relevance of member state sovereignty within the European legal order.

The emergence of the e-Evidence system has generated extensive academic and institutional debate regarding its implications for the allocation of powers between the European Union and its member states. While proponents emphasise the necessity of modernising investigative instruments in response to technological developments, critics have questioned whether direct cross-border access to electronic evidence may diminish the traditional role of national authorities and weaken procedural safeguards rooted in national constitutional traditions. The discussion is particularly relevant because judicial cooperation in criminal matters remains a sensitive domain closely connected with the exercise of sovereign powers, the protection of fundamental rights, and the administration of criminal justice. Consequently, the e-Evidence framework provides an appropriate case study through which to examine broader trends affecting the constitutional architecture of the European Union and the evolving concept of sovereignty in an increasingly integrated legal space.

This article examines the legal and constitutional implications of the e-Evidence system from the perspective of European Union law. It seeks to answer the following research question: *To what extent does the e-Evidence system affect the principle of member state sovereignty within the framework of judicial cooperation in criminal matters in the European Union?* In order to address this question, the article employs doctrinal legal analysis, supplemented by comparative and analytical methods. Particular attention is devoted to the legal framework of e-Evidence, its relationship with traditional mechanisms of judicial cooperation, its impact upon the sovereign powers of member states, and the safeguards designed to protect fundamental rights. On the basis of this analysis, the article formulates conclusions concerning the future development of digital judicial cooperation within the European Union and presents selected considerations regarding possible future development.

The research is primarily based on the doctrinal method of legal analysis, which is applied to examine the relevant legal framework governing the acquisition of electronic evidence within the European Union. Particular attention is devoted to the interpretation

---

[5] See, for example: E-evidence – Cross-Border Access to Electronic Evidence.

of primary and secondary European Union legislation, as well as related legislative and policy documents issued by the European institutions. The analysis also takes into account the broader constitutional principles governing the *Area of Freedom, Security, and Justice*, including mutual trust, mutual recognition, proportionality, and respect for fundamental rights. The doctrinal analysis is complemented by analytical and comparative methods. The analytical method is employed to assess the legal implications of the e-Evidence framework for judicial cooperation in criminal matters and for the exercise of member state sovereignty. The comparative method is used to contrast the e-Evidence system with traditional mechanisms of judicial cooperation, particularly mutual legal assistance and instruments based on the principle of mutual recognition. Through the combination of these methods and sources, the article seeks to provide a comprehensive assessment of the legal and constitutional implications of the e-Evidence framework within the evolving system of European criminal justice.

## THE CONCEPT OF *ELECTRONIC EVIDENCE* AND ITS SIGNIFICANCE IN THE DIGITAL SOCIETY

The rapid digitalisation of contemporary society has fundamentally transformed the manner in which individuals communicate, conduct business, and interact with public authorities. Virtually every aspect of modern life now generates digital traces capable of revealing information concerning human behaviour, social relationships, and economic activities.[6] This development has inevitably affected criminal proceedings, where evidentiary material is increasingly derived from electronic devices, communication networks, and digital platforms. As criminal activities have likewise adapted to the digital environment, electronic evidence has become an indispensable component of the investigation and prosecution of both conventional and cyber-enabled criminal offences.[7] Consequently, electronic evidence has acquired considerable practical and theoretical significance within European criminal justice systems and has emerged as a central element of contemporary judicial cooperation in criminal matters.

Despite its growing importance, no universally accepted definition of *electronic evidence* exists in legal doctrine or within international and European legal instruments. The absence of a universally accepted definition is also reflected in comparative legal scholarship. Some authors distinguish between the concepts of *electronic information*,

---

6 MIFSUD BONNICI, J. P. – TUDORICA, M. – CANNATACI, J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. In: BIASIOTTI, M. A. – MIFSUD BONNICI, J. P. – CANNATACI, J. – TURCHI, F. (eds.). *Handling and Exchanging Electronic Evidence Across Europe*. Cham: Springer, 2018, pp. 189–190.

7 Ibid., pp. 190–191; FRANSSEN, V. Cross-Border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation Under the e-Evidence Regulation. In: MITSILEGAS, V. – BERGSTRÖM, M. – QUINTEL, T. (eds.). *Research Handbook on EU Criminal Law*. Cheltenham: Edward Elgar Publishing, 2024, pp. 184–185; TOSZA, S. All Evidence Is Equal, But Electronic Evidence Is More Equal Than Any Other. *New Journal of European Criminal Law* [online]. 2020, Vol. 11, No. 2, pp. 161–183 [cit. 2026-05-20]. Available at: https://journals.sagepub.com/doi/full/10.1177/2032284420919802.

*electronic evidence*, and *digital information*, arguing that the latter more accurately describes information existing in digital form irrespective of the medium through which it is stored or transmitted. It should not be overlooked that the concept of *electronic evidence* last decades has been generally understood as encompassing information of evidential value that is stored, processed, generated, or transmitted in digital form.[8] Such information may originate from computers, mobile telephones, cloud services, social networking platforms, or electronic communications systems. Unlike traditional forms of evidence, electronic evidence is characterised by its intangible nature, technological dependence, and potential volatility. Similar observations may be found beyond the European legal context.[9] Digital information can be altered, transferred, or deleted within seconds and may simultaneously exist in multiple jurisdictions.[10] These characteristics necessitate specialised legal mechanisms capable of ensuring its effective acquisition, preservation, and admissibility in criminal proceedings.

The growing significance of electronic evidence reflects broader structural changes within modern societies. Economic activity, public administration, and interpersonal communication increasingly rely upon digital infrastructures operated by private entities whose activities transcend national borders. As a result, information relevant to criminal investigations is often held by service providers established in another member state or outside the European Union. This situation has created growing tensions between the protection of personal data and the operational need of law enforcement authorities to obtain access to electronic evidence stored or controlled across borders, particularly in cloud computing environments.[11] This phenomenon has weakened the

---

[8] KERR, O. S. Digital Evidence and the New Criminal Procedure. *Columbia Law Review*. 2005, Vol. 105, No. 1, pp. 279–318; PAUL, G. L. *Foundations of Digital Evidence*. Chicago: American Bar Association, 2008; MARSHALL, A. *Digital Forensics: Digital Evidence in Criminal Investigations*. Chichester: John Wiley & Sons, 2009; SCANLAN, D. M. *Digital Evidence in Criminal Law*. Toronto: Canada Law Book, 2011; BIASIOTTI – MIFSUD BONNICI – CANNATACI – TURCHI (eds.), *c. d.*; MASON, S. – SENG, D. (eds.). *Electronic Evidence and Electronic Signatures*. 5th ed. London: University of London Press, 2021.

[9] See, for example: ANGEL, O. E. M. et al. Digital Evidence as a Means of Proof in Criminal Proceedings. *Russian Law Journal*. 2023, Vol. 11, No. 5, pp. 96–105; SHULHA, V. – KALIUZHNA, L. Electronic Evidence in Criminal Procedure: Methods for Its Detection, Investigation and Legal Consolidation. *Theory and Practice of Forensic Science and Criminalistics* [online]. 2025, Vol. 40, No. 3, pp. 136–152 [cit. 2026-05-20]. Available at: https://doi.org/10.32353/khrife.3.2025.10; FOMINA, T. H. – RACHYNSKYI, O. O. Електронні докази у кримінальному процесі: проблемні питання теорії та практики [Electronic Evidence in Criminal Proceedings: Problematic Issues of Theory and Practice]. *Вісник Харківського національного університету внутрішніх справ* [Bulletin of Kharkiv National University of Internal Affairs] [online]. 2023, Vol. 102, No. 3, pp. 207–220 [cit. 2026-05-20]. Available at: https://doi.org/10.32631/v.2023.3.43; ALRAGGAD, M. M. – ALMAHASNEH, A. A. A. A. – BOROVIKOVA, V. – ZHYVKO, Z. – KOMISSARCHUK, Y. The Policy of Rethinking the Criminal Process in the National Security System: The Impact of Digitalisation on Working with Electronic Evidence. *Social & Legal Studios* [online]. 2024, Vol. 7, No. 2, pp. 162–170 [cit. 2026-05-20]. Available at: https://doi.org/10.32518/sals2.2024.162.

[10] MIFSUD BONNICI – TUDORICA – CANNATACI, *c. d.*, pp. 190–198; WARKEN, C. Classification of Electronic Data for Criminal Law Purposes. *eucrim* [online]. 2018, Vol. 13, No. 4, pp. 226–234 [cit. 2026-05-20]. Available at: https://doi.org/10.30709/eucrim-2018-023.

[11] SHURSON, J. Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts Between EU and US Law. *International Journal of Law and Information Technology*. 2020, Vol. 28, No. 2, pp. 167–184.

practical relevance of territorial boundaries that have traditionally shaped criminal jurisdiction and judicial cooperation. Whereas physical evidence is usually linked to a specific *location*, electronic evidence may be distributed across multiple jurisdictions without any meaningful connection to territorial concepts traditionally associated with sovereign authority.

The significance of electronic evidence extends beyond investigative efficiency. Although the practical importance of electronic evidence is widely acknowledged, its growing role also requires a more nuanced legal assessment. The increasing dependence of criminal investigations upon electronically stored data does not merely expand the range of available evidentiary sources but fundamentally alters the relationship between investigative powers, private actors, and individual rights. Unlike traditional forms of evidence, electronic data is commonly generated, processed, and retained by private service providers operating across multiple jurisdictions. Consequently, the effectiveness of criminal proceedings increasingly depends upon the willingness and legal obligation of private entities to cooperate with public authorities. This development illustrates that the legal regulation of electronic evidence is no longer concerned solely with procedural efficiency but also with redefining the institutional balance between public authority, private digital infrastructure, and the constitutional guarantees protecting individuals within the European legal order. Its acquisition and use directly affect fundamental constitutional values, including the protection of private life, personal data, and procedural fairness.[12] Access to digital information may enable authorities to obtain detailed insights into an individual's activities, thereby creating a heightened risk of disproportionate interference with fundamental rights. At the same time, the inability to obtain electronic evidence promptly may seriously undermine criminal investigations. Modern legal systems are therefore required to balance the effective administration of criminal justice with the protection of fundamental rights within a society governed by the rule of law.

Within the European Union, the increasing reliance upon electronic evidence has also exposed limitations of traditional mechanisms of judicial cooperation in criminal matters. The transnational character of digital information frequently results in situations where evidence relevant to a criminal investigation is controlled by a service provider operating across several jurisdictions. Such circumstances have demonstrated the inadequacy of procedures originally designed for the exchange of physical evidence between sovereign states.[13] Consequently, the emergence of electronic evidence has stimulated the development of innovative legal instruments aimed at *modernising judicial cooperation* within the *Area of Freedom, Security, and Justice*. The e-Evidence framework represents an attempt to adapt European criminal justice to the realities of the digital age.

---

[12] VOGLER, R. Criminal Evidence and Respect for Fair Trial Guarantees in the Dialogue Between the European Court of Human Rights and National Courts. In: RUGGERI, S. (ed.). *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-Border Cases*. Cham: Springer, 2014, pp. 181–192.

[13] MIFSUD BONNICI – TUDORICA – CANNATACI, *c. d.*, pp. 194–196; FRANSSEN, *c. d.*, pp. 184–211.

## TRADITIONAL MECHANISMS FOR OBTAINING ELECTRONIC EVIDENCE IN CROSS-BORDER CASES

Prior to the adoption of the e-Evidence framework, the acquisition of electronic evidence in cross-border criminal investigations was governed primarily by traditional mechanisms of international judicial cooperation. These mechanisms reflected the classical principles of public international law and criminal procedure,[14] according to which coercive powers were closely linked to territorial sovereignty. Consequently, authorities of one state were generally prohibited from directly obtaining evidence located within another state's jurisdiction. Instead, evidence had to be requested through competent authorities of the requested state. Although these mechanisms were originally designed for conventional forms of evidence, they were subsequently applied to electronic evidence despite the distinct characteristics of digital information.

The principal instrument was *mutual legal assistance*, which has long constituted the cornerstone of international cooperation in criminal matters. Under this model, a judicial or prosecutorial authority seeking evidence abroad submits a formal request to the competent authority of another state, which evaluates and executes the request in accordance with domestic law. Within Europe, mutual legal assistance developed through a network of bilateral treaties, multilateral conventions, and European Union instruments.[15] Despite its importance, the system was frequently criticised for procedural complexity, administrative burdens, and excessive delays. Requests often required translation, transmission through multiple authorities, and compliance with differing procedural requirements, thereby reducing the effectiveness of investigations involving rapidly changing digital information.

The emergence of electronic evidence exposed these shortcomings more acutely than any previous category of evidence. Unlike physical objects, electronic data may be altered, transferred, or deleted within a short period of time, making delays particularly problematic. Moreover, electronic evidence is often controlled by private service providers whose operations span multiple jurisdictions. Determining the location of the requested data may itself prove difficult, especially where cloud computing technologies distribute information across several states. These circumstances revealed a growing mismatch between territorially oriented cooperation mechanisms and the realities of digital communications infrastructure.

In response, the European Union progressively developed instruments based upon the principle of *mutual recognition*. The European Investigation Order represented one of the most significant examples of this approach, providing a more streamlined

---

[14] See, for example: SLUITER, G. – FRIMAN, H. – LINTON, S. – VASILIEV, S. – ZAPPALÀ, S. (eds.). *International Criminal Procedure: Principles and Rules*. Oxford: Oxford University Press, 2013.

[15] HECKER, B. Europäisches Strafrecht Post-Lissabon. In: AMBOS, K. (ed.). *Europäisches Strafrecht Post-Lissabon*. Göttingen: Universitätsverlag Göttingen, 2011, pp. 15–16; KLIMEK, L. *Základy trestného práva Európskej únie* [Fundamentals of European Union Criminal Law]. Bratislava: Wolters Kluwer, 2017, pp. 157–160.

framework for obtaining evidence across borders.[16] Nevertheless, it remained dependent upon cooperation between national authorities and continued to be influenced by territorial considerations and domestic procedural requirements. Although mutual recognition improved efficiency, it did not eliminate the structural difficulties associated with obtaining electronic evidence from foreign jurisdictions.

A further challenge resulted from the increasing concentration of electronic data in the hands of private service providers, many headquartered outside the member state conducting the investigation. Authorities frequently relied on voluntary cooperation with such providers, but this approach lacked a harmonised legal basis and often generated legal uncertainty. Service providers were confronted with potentially conflicting obligations concerning data protection, privacy, and disclosure requirements. Consequently, voluntary cooperation could not provide a comprehensive solution to the growing demand for cross-border access to electronic evidence.

The limitations of traditional mechanisms demonstrated that the existing legal framework had been developed for a technological environment substantially different from that of the twenty-first century. Although *mutual legal assistance* and *mutual recognition* remain indispensable components of judicial cooperation in criminal matters, their design was primarily based upon assumptions concerning physical evidence and territorially defined investigative powers. The increasingly borderless nature of digital information challenged these assumptions and created pressure for new legal instruments capable of ensuring both efficiency and legal certainty. From a broader constitutional perspective, however, the limitations of traditional mechanisms should not be understood solely as a consequence of technological progress. Rather, they reveal structural constraints inherent in a model of judicial cooperation founded primarily upon territorial jurisdiction and inter-state communication. Mutual legal assistance and, to a lesser extent, mutual recognition were developed within a legal environment in which evidence was generally linked to a clearly identifiable territory and remained under the effective control of public authorities. Electronic data fundamentally challenges these assumptions because its location, control, and accessibility frequently transcend territorial boundaries. Consequently, the difficulties encountered in obtaining electronic evidence do not merely demonstrate the practical shortcomings of existing procedural instruments but also illustrate the growing divergence between territorially oriented legal concepts and the realities of the digital environment. The emergence of the e-Evidence framework may therefore be regarded as a response not only to operational needs but also to a gradual transformation in the conceptual foundations of judicial cooperation in criminal matters. It was within this context that the European Union adopted the e-Evidence framework, which represents an attempt to adapt judicial cooperation to the realities of the digital age.

---

[16] KLIMEK, *Mutual Recognition of Judicial Decisions in European Criminal Law*, pp. 421–459; TOSZA, *c. d.*, pp. 161–183; SIGNORATO, S. Cross-Border Gathering of E-Evidence: Different Legal Frameworks in European Union and Council of Europe. *Journal of Eastern European Criminal Law*. 2023, Vol. 10, No. 1, pp. 9–18.

## THE LEGAL FRAMEWORK OF E-EVIDENCE IN THE EUROPEAN UNION

The adoption of the e-Evidence framework represents one of the most significant legislative developments in the field of judicial cooperation in criminal matters within the European Union in recent years. It reflects the European Union's response to the increasing challenges associated with obtaining electronic evidence in a digital environment characterised by cross-border data flows, cloud computing, and the global operation of online service providers. The legislative initiative[17] was driven by the recognition that traditional mechanisms of mutual legal assistance and mutual recognition were frequently unable to provide timely access to electronic data required for criminal investigations and prosecutions. The resulting delays often undermined the effectiveness of criminal proceedings and created practical obstacles for authorities seeking to combat serious forms of crime with a substantial digital dimension. Against this background, the European Union sought to establish a more efficient legal framework capable of reconciling the needs of effective law enforcement with the protection of fundamental rights and the preservation of legal certainty.

The legal basis for the e-Evidence framework is found primarily in Article 82(1)(d) and Article 87(2)(a) of the *Treaty on the Functioning of the European Union*,[18] which empower the European Union to adopt measures facilitating judicial cooperation in criminal matters and cooperation between law enforcement authorities. These provisions form part of the broader constitutional framework governing the *Area of Freedom, Security and Justice*, within which judicial cooperation is founded upon the principles of *mutual trust* and *mutual recognition*.[19] The e-Evidence framework must therefore be understood not as an isolated legislative measure but as a component of the continuing evolution of European criminal justice. Its adoption reflects the increasing willingness of the European Union to develop mechanisms capable of responding to technological developments that challenge traditional territorial models of criminal procedure and evidentiary cooperation.

The central component of the e-Evidence framework is the *Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for*

---

[17] See: European 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. In: *EUR-Lex: Access to European Union Law* [online]. Brussels, 17. 4. 2018 [cit. 2026-05-22]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018PC0225; see also: European Commission. Commission Staff Working Document. Impact Assessment Accompanying the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and the Proposal for a Directive Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings. SWD(2018) 118 final. In: *EUR-Lex: Access to European Union Law* [online]. Brussels, 17. 4. 2018 [cit. 2026-05-22]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018SC0118.

[18] Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union* [online]. C 326, 26. 10. 2012, p. 47 [cit. 2026-05-22]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

[19] KLIMEK, *Mutual Recognition of Judicial Decisions in European Criminal Law*, pp. 103–134.

*electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*.[20] The Regulation introduces two novel legal instruments designed specifically for the acquisition of electronic evidence across borders within the European Union. The *European Production Order* enables a competent authority of one member state to require a service provider established or represented in another member state to produce specified categories of electronic data directly. The *European Preservation Order*, by contrast, obliges the service provider to preserve the requested data for a defined period in order to prevent its alteration, deletion or loss pending subsequent procedural measures. Both instruments seek to ensure rapid access to relevant information while maintaining procedural safeguards intended to protect affected persons and preserve the rule of law.[21]

The Regulation distinguishes between several categories of electronic data, including subscriber data, traffic data, transactional data, and content data. This distinction is of considerable legal significance because the degree of interference with fundamental rights varies according to the nature of the information sought. Subscriber data is generally subject to less restrictive conditions, whereas access to traffic, transactional, and content data requires enhanced procedural safeguards due to their greater potential impact upon privacy and confidentiality of communications. The Regulation accordingly establishes differentiated conditions for issuing orders, specifies the authorities competent to issue them, and introduces mechanisms designed to ensure proportionality and judicial oversight. Through this approach, the European legislature sought to balance investigative effectiveness against the protection of fundamental rights guaranteed under the Charter of Fundamental Rights of the European Union.

The effectiveness of the Regulation (EU) 2023/1543 is reinforced by the *Directive (EU) 2023/1544 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*.[22] The Directive addresses a practical obstacle that had long complicated the acquisition of electronic evidence, namely the absence of clearly identifiable entities capable of receiving and responding to legally binding requests. It requires certain service providers offering services within the

---

[20] 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. *Official Journal of the European Union* [online]. 28. 7. 2023, L 191, pp. 118–180 [cit. 2026-05-22]. Available at: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng.

[21] POLYZOIDOU, V. e-Evidence Regulation: A Contemporary Trojan Horse in Criminal Proceedings? In: SYNODINOU, T.-E. et al. (eds.). *EU Digital Law in the AI Era*. Cham: Springer, 2025, pp. 239–261 [cit. 2026-05-20]. Available at: https://doi.org/10.1007/978-3-031-96743-6_13; TURANJANIN, V. EncroChat, Sky ECC and Regulation (EU) 2023/1543: Towards a New Standards of Digital Evidence (I). *Journal of Criminology and Criminal Law*. 2025, Vol. 63, No. 3, pp. 7–30.

[22] 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. *Official Journal of the European Union* [online]. L 191, 28. 7. 2023, pp. 181–190 [cit. 2026-05-22]. Available at: https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng.

European Union to designate an establishment or appoint a legal representative responsible for receiving, complying with and enforcing decisions relating to electronic evidence. The Directive thereby complements the Regulation by creating the institutional infrastructure necessary for the practical operation of the new system. Together, the Regulation and the Directive form a coherent legislative package intended to facilitate direct and efficient cooperation between competent authorities and private service providers. Beyond its procedural innovations, the e-Evidence framework also reflects a broader evolution of European criminal justice. Rather than merely simplifying existing mechanisms, it introduces a regulatory model that seeks to reconcile the effectiveness of cross-border investigations with the constitutional principles governing judicial cooperation within the European Union. Its long-term significance will therefore depend not only upon its practical efficiency but also upon its ability to maintain an appropriate balance between effective law enforcement, legal certainty, and the protection of fundamental rights.

One of the most innovative features of the e-Evidence framework is the establishment of a model based upon direct cooperation with service providers. Under traditional mechanisms, requests for evidence were generally transmitted through public authorities of the state in which the evidence was located. The new framework significantly reduces the role of intermediary state authorities by permitting direct communication between the issuing authority and the service provider. This approach is intended to accelerate access to electronic evidence and reduce procedural burdens associated with cross-border cooperation. At the same time, however, it represents a substantial departure from conventional models of judicial cooperation based upon territorial sovereignty and inter-state interaction. The practical implementation of this model may nevertheless present a number of challenges. In particular, competent authorities and service providers may encounter difficulties in determining the applicable procedural requirements where electronic data is linked to several jurisdictions simultaneously. Questions may also arise concerning the coordination of parallel proceedings, compliance with different national procedural standards, and the timely execution of legally binding orders. Although the Regulation establishes a harmonised legal framework, its effective operation will inevitably depend upon consistent administrative practice and close cooperation between the authorities involved. The legal implications of this transformation extend beyond procedural efficiency and raise broader questions concerning the evolving relationship between member states, European Union institutions, and private actors within the administration of criminal justice.

The e-Evidence framework should therefore be regarded as more than a technical legislative response to technological developments. It constitutes an important stage in the evolution of judicial cooperation in criminal matters and reflects broader trends towards the digitalisation and integration of criminal justice within the European Union. By introducing legally binding mechanisms for the direct acquisition and preservation of electronic evidence, the framework seeks to address practical deficiencies of existing cooperation instruments while preserving the fundamental values underpinning the European legal order. Nevertheless, there can be little doubt that the adoption of the Regulation (EU) 2023/1543 and the Directive (EU) 2023/1544 marks a significant

development in the constitutional and procedural landscape of European judicial cooperation.

At the same time, the new legal framework cannot be regarded as free from controversy. While its primary objective is to improve the efficiency of cross-border investigations, the introduction of direct obligations for private service providers inevitably raises questions concerning the allocation of legal responsibilities between public authorities and private actors. Service providers may be required to assess the formal validity of orders and to comply with obligations originating from different legal systems, potentially exposing them to conflicting legal duties. Although the Regulation contains procedural safeguards intended to minimise such risks, its practical effectiveness will ultimately depend upon consistent implementation by competent authorities and constructive cooperation between public institutions and private entities operating within the digital environment.

## THE IMPACT OF THE E-EVIDENCE SYSTEM ON THE SOVEREIGNTY OF MEMBER STATES

The introduction of the e-Evidence framework opens debate regarding its implications for member state sovereignty within the European Union. Judicial cooperation in criminal matters has traditionally been regarded as a core manifestation of sovereign authority because it concerns the investigation, prosecution and punishment of criminal conduct. Consequently, legislative developments that alter the manner in which authorities cooperate across borders inevitably raise questions concerning the role of member states within the European system of criminal justice. By enabling authorities of one member state to address legally binding orders directly to private entities operating in another member state, the e-Evidence framework challenges assumptions underlying traditional models of judicial cooperation. More broadly, it should be not overlooked that European criminal law has evolved within a continuing tension between the deepening of supranational cooperation and the preservation of member states' sovereignty in criminal matters. The development of instruments based on mutual recognition reflects an effort to reconcile these competing objectives within the *Area of Freedom, Security, and Justice*.[23]

Sovereignty remains a foundational concept of public and international law.[24] Traditionally, it denotes the supreme authority of a state to regulate affairs within its territory and exercise public powers independently of external interference. Within the European Union, however, sovereignty has evolved through the transfer of certain competences to the Union and the acceptance of limitations upon unilateral state action. As a result,

---

[23] HECKER, *Európäisches Strafrecht Post-Lissabon*, pp. 13–15; KLIMEK, *Základy trestného práva Európskej únie* [Fundamentals of European Union Criminal Law], pp. 150–160; BÖSE (ed.). *c. d.*, pp. 673–706.

[24] See, for example: ROSE, C. – BLOKKER, N. – DAM-DE JONG, D. – VAN DEN DRIEST, S. – HEINSCH, R. – KOPPE, E. – SCHRIJVER, N. *An Introduction to Public International Law*. Cambridge: Cambridge University Press, 2022.

sovereignty increasingly operates within a framework of shared competences, mutual obligations and institutional cooperation.[25] Judicial cooperation in criminal matters provides a particularly clear example of this transformation.

From this perspective, the e-Evidence framework represents a further stage in the evolution of sovereignty within the *Area of Freedom, Security*, *and Justice*. Traditional mutual legal assistance procedures relied upon interaction between state authorities, with the requested state exercising substantial control over the execution of requests. By contrast, the e-Evidence framework reduces the procedural role of the state in which the service provider is established or represented, allowing competent authorities to communicate directly with providers.[26] At first sight, this development appears to limit the ability of member states to supervise investigative measures affecting entities within their jurisdiction and has therefore been viewed by some commentators as a departure from traditional manifestations of territorial sovereignty.

A closer examination, however, reveals a more nuanced picture. The framework does not grant unlimited powers to issuing authorities and does not entirely exclude the involvement of other member states. Regulation (EU) 2023/1543 establishes procedural safeguards, notification mechanisms and grounds for challenging or restricting execution. Moreover, the framework derives its legitimacy from legislation adopted through the constitutional procedures of the European Union and accepted by participating member states. The resulting limitations upon unilateral state control therefore arise from the collective exercise of legislative authority rather than external interference. In this sense, the framework reflects a reconfiguration rather than a negation of sovereignty. Nevertheless, this conclusion is not universally accepted within academic literature. Some commentators argue that the reduced procedural involvement of the executing member state may weaken traditional mechanisms of national control over investigative measures affecting persons and entities within its jurisdiction. Others maintain that such developments merely represent a logical continuation of the principle of mutual recognition and reflect the increasing integration of judicial cooperation within the *Area of Freedom, Security, and Justice*. The latter interpretation appears more persuasive, as the powers exercised under the e-Evidence framework derive from a common legislative framework adopted collectively by the member states rather than from unilateral assertions of authority by individual national authorities.

Particular attention must be paid to the relationship between sovereignty and digital information. Traditional concepts of territoriality were developed in an environment where persons, property, and evidence could generally be linked to a specific location. Electronic data challenge these assumptions because they may exist simultaneously in multiple jurisdictions and are often detached from any meaningful territorial connection.

---

[25] See, for example: BARNARD, C. – PEERS, S. (eds.). *European Union Law*. 4th ed. Oxford: Oxford University Press, 2023.

[26] SACHOULIDOU, A. 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. *New Journal of European Criminal Law* [online]. 2024, Vol. 15, No. 3, pp. 256–274 [cit. 2026-05-20]. Available at: https://doi.org/10.1177/2032284424125864.

The e-Evidence framework may therefore be viewed as an attempt to adapt legal mechanisms to technological realities rather than as an effort to diminish the constitutional position of member states. By facilitating access to electronic data through regulated procedures, it addresses practical obstacles resulting from the increasingly borderless nature of digital information.

The constitutional significance of the e-Evidence framework lies in its contribution to a more integrated model of judicial cooperation. Whereas traditional mechanisms emphasised cooperation between sovereign states, the new framework places greater emphasis upon cooperation within a common legal area founded upon mutual trust and shared legal standards. This development reflects broader trends observable across European criminal justice, including mutual recognition instruments, *Eurojust*, and the *European Public Prosecutor's Office*. The e-Evidence framework therefore forms part of a wider constitutional evolution characterised by the adaptation of sovereign powers to the requirements of an integrated legal order.

Accordingly, the impact of the e-Evidence system on member state sovereignty should not be understood solely in terms of limitation or erosion. While the framework reduces certain traditional manifestations of territorial control, it simultaneously strengthens the collective capacity of member states to combat cross-border criminality. The resulting transformation may be described as a shift from a purely state-centred model of sovereignty towards a model of cooperative sovereignty exercised through the institutions and legal mechanisms of the European Union. The key issue is therefore not whether sovereignty has been weakened, but how its exercise has been redefined in response to digitalisation and European integration.

## THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE OBTAINING OF ELECTRONIC EVIDENCE

The increasing reliance upon electronic evidence in criminal proceedings has intensified the need to ensure effective protection of fundamental rights within the European Union. The legal regulation of cross-border access to electronic evidence increasingly reflects a structural tension between data protection regimes and the investigative needs of law enforcement authorities, particularly where data is controlled by service providers operating across multiple jurisdictions.[27] While digital technologies have enhanced the ability of competent authorities to investigate and prosecute criminal offences, they have also increased the potential for interference with individual rights and freedoms. Electronic evidence frequently contains sensitive information concerning personal communications, social relationships, professional activities, and financial transactions. Consequently, its acquisition lies at the intersection of two legitimate objectives: the effective administration of criminal justice and the protection of fundamental rights guaranteed under the constitutional traditions of the member states,

[27] SHURSON, *c. d.*, pp. 167–170.

the Convention for the Protection of Human Rights and Fundamental Freedoms[28] (European Convention on Human Rights) and the *Charter of Fundamental Rights of the European Union*.[29]

Among the rights most directly affected are the right to respect for private and family life and the right to the protection of personal data. Access to subscriber data, traffic data, transactional data, or content data may reveal significant information about an individual's behaviour, associations, and communications. The distinction between these categories is therefore not merely technical but closely linked to the degree of interference with protected rights. While subscriber data generally involves a lower level of intrusion, access to content data may disclose the substance of private communications and thus require a higher level of protection.[30] The legal framework governing electronic evidence must accordingly ensure that investigative powers are exercised only for legitimate purposes and subject to adequate safeguards. Although the e-Evidence framework itself has not yet generated a substantial body of judicial interpretation, its future application will necessarily be influenced by the (future) case law of the Court of Justice of the European Union.

The principle of proportionality plays a central role in this context. As a general principle of European Union law, it requires that measures interfering with fundamental rights pursue a legitimate objective, be necessary, and maintain an appropriate balance between competing interests.[31] Within the field of electronic evidence, proportionality requires consideration of the seriousness of the offence, the nature of the data sought, and the degree of intrusion involved. The e-Evidence framework reflects this principle by establishing differentiated procedural requirements according to the category of electronic data concerned and by imposing conditions on the issuance of *European Production Orders* and *European Preservation Orders*.

Judicial protection constitutes an equally important safeguard. Individuals affected by investigative measures must have access to effective legal remedies capable of challenging the legality and proportionality of interferences with their rights. This requirement is particularly significant in cross-border situations where the issuing authority, service provider, and affected individual may be located in different jurisdictions. The e-Evidence framework seeks to address these challenges through procedural mechanisms intended to ensure accountability and legal certainty. From a practical perspective, particular difficulties may arise in situations involving several affected jurisdictions or complex digital infrastructures. The exercise of procedural rights may become more demanding where the issuing authority, the service provider and the person concerned

---

28 European Court of Human Rights, Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols Nos. 11, 14 and 15* [online]. Strasbourg [cit. 2026-05-22]. Available at: https://www.echr.coe.int/documents/d/echr/convention_eng.

29 Charter of Fundamental Rights of the European Union. *Official Journal of the European Union* [online]. C 202, 7. 6. 2016, pp. 389–405 [cit. 2026-05-22]. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

30 SACHOULIDOU, *c. d.*, pp. 256–274.

31 GONZÁLEZ FUSTER, G. – VÁZQUEZ MAYMIR, S. *Cross-Border Access to E-Evidence: Framing the Evidence*. CEPS Papers in Liberty and Security in Europe, No. 2020-02. Brussels, February 2020.

are located in different member states, each operating under distinct procedural rules. Ensuring that affected individuals are able to exercise available remedies effectively and within appropriate time limits may therefore represent one of the principal challenges accompanying the practical application of the e-Evidence framework.

Nevertheless, the practical effectiveness of these safeguards remains dependent upon their implementation by national authorities and their interpretation by courts at both national and European levels. The protection of fundamental rights is further complicated by the growing role of private service providers. Electronic evidence is frequently controlled by private entities operating across multiple jurisdictions and subject to potentially conflicting legal obligations concerning privacy, data protection, and disclosure. The e-Evidence framework attempts to provide legal certainty by defining the obligations of service providers and establishing harmonised procedures for responding to requests from competent authorities. Nevertheless, legislative harmonisation alone cannot guarantee the effective protection of fundamental rights. The practical operation of the e-Evidence framework will largely depend upon the manner in which competent authorities apply the principles of necessity and proportionality in individual cases, as well as upon the availability of effective judicial review. Given the recent adoption of the legislative framework, many questions concerning its practical interpretation remain open and are likely to be clarified only through future judicial practice. The long-term legitimacy of the e-Evidence system will therefore depend not only upon its capacity to facilitate criminal investigations but equally upon its ability to ensure a consistent and effective standard of fundamental rights protection throughout the European Union.

However, the increasing involvement of private actors continues to raise questions concerning accountability and the balance between public authority and private participation in criminal justice.

Particular importance must also be attached to the principle of legal certainty. Individuals should be able to foresee the circumstances under which authorities may obtain access to their electronic data and the safeguards available against abuse. This requires clear legislative provisions, transparent procedures, and effective oversight mechanisms. Without such safeguards, the increasing use of electronic evidence could undermine public confidence in both criminal justice systems and the broader legal order.

In addition, the protection of fundamental rights constitutes one of the principal tests of the legitimacy of the e-Evidence framework. Although improving access to electronic evidence is necessary for combating serious forms of criminality, investigative effectiveness cannot be pursued at the expense of the values upon which the European legal order is founded. The long-term success of the e-Evidence system will therefore depend upon its ability to maintain an appropriate balance between investigative efficiency and individual rights. In this respect, the protection of fundamental rights should be regarded not as an obstacle to judicial cooperation but as a necessary condition for its legitimacy and sustainability.

## THE RELATIONSHIP BETWEEN E-EVIDENCE, EUROJUST, EUROPOL, AND THE EUROPEAN JUDICIAL NETWORK

The e-Evidence framework does not operate in isolation within the institutional architecture of the European Union. Rather, it forms part of a broader system of judicial and law enforcement cooperation designed to facilitate the prevention, investigation, and prosecution of criminal offences with a cross-border dimension. The effectiveness of the new framework is therefore closely connected with the activities of existing European bodies and networks, particularly *Eurojust*, *Europol*, and the *European Judicial Network*. Although these entities perform distinct functions and are governed by separate legal instruments, they collectively contribute to the functioning of the *Area of Freedom, Security, and Justice* and support the practical implementation of judicial cooperation in criminal matters. Understanding the relationship between e-Evidence and these established mechanisms is essential for assessing the position of the new framework within the wider structure of European criminal justice.

First, *Eurojust* occupies a particularly significant position in this context. Established to strengthen coordination and cooperation between national judicial authorities, Eurojust assists member states in the investigation and prosecution of serious cross-border criminality. Its activities include facilitating the exchange of information, resolving conflicts of jurisdiction, supporting the execution of mutual legal assistance requests, and coordinating complex multinational investigations.[32] Although the e-Evidence framework introduces mechanisms that reduce reliance upon traditional forms of inter-state cooperation, it does not eliminate the need for judicial coordination. On the contrary, situations involving multiple jurisdictions, competing investigative interests, or parallel criminal proceedings may continue to require the involvement of Eurojust. The increasing use of electronic evidence is likely to generate new forms of legal complexity, particularly where investigative measures affect several member states simultaneously. Such situations may require more intensive coordination than under traditional forms of judicial cooperation. Parallel investigations, overlapping jurisdictional interests, and differing national procedural approaches may increase the need for timely communication between the competent authorities concerned. In this respect, the institutional support provided by Eurojust may become particularly valuable in preventing unnecessary procedural conflicts and promoting coherent handling of complex cross-border investigations involving electronic evidence. In such circumstances, Eurojust remains an important institution for ensuring coherent and effective judicial cooperation.

Second, the relationship between e-Evidence and *Europol* is equally significant. Unlike Eurojust, which primarily supports judicial authorities, Europol functions as the European Union Agency for Law Enforcement Cooperation and provides operational assistance to competent law enforcement authorities. Its role includes the collection, analysis, and exchange of criminal intelligence, the support of operational activities

---

[32] AMBOS, *c. d.*, p. 563 et seq.; BÖSE (ed.), *c. d.*, p. 1074 et seq.; HECKER, B. *Europäisches Strafrecht*. 7. Aufl. Berlin, Heidelberg: Springer, 2025, p. 171 et seq.

and the development of specialised expertise concerning emerging forms of criminality.[33] The growing importance of electronic evidence is closely linked to technological developments that also influence Europol's activities, particularly in the fields of cybercrime, organised crime, and terrorism. Through its analytical capacities and specialised knowledge, Europol contributes to the identification of digital evidence and supports investigations that may subsequently require the use of instruments provided by the e-Evidence framework. Consequently, the relationship between Europol and e-Evidence may be characterised as complementary, with the former facilitating the identification and analysis of information and the latter providing legal mechanisms for obtaining evidence relevant to criminal proceedings.

Third, particular attention should also be devoted to the *European Judicial Network*. Established to facilitate direct contacts between national judicial authorities, the Network serves as a practical instrument for improving cooperation in criminal matters across the European Union. It provides information regarding national legal systems, assists in identifying competent authorities, and supports the resolution of practical difficulties arising in cross-border cases.[34] Although the e-Evidence framework introduces a more direct model of cooperation involving service providers, national authorities may continue to encounter legal and procedural questions requiring clarification. Differences in domestic procedural rules, constitutional requirements, and legal traditions have not disappeared with the adoption of the new framework. The European Judicial Network therefore retains an important role as a mechanism for communication, consultation, and practical assistance. Its activities contribute to the effective operation of the broader system of judicial cooperation within which e-Evidence functions.

The introduction of e-Evidence should not be interpreted as replacing existing instruments and institutions but rather as complementing them. Traditional mechanisms of cooperation remain necessary in numerous situations, particularly where investigative measures extend beyond the categories of electronic evidence covered by the Regulation or involve jurisdictions outside the European Union. Likewise, the coordination functions performed by Eurojust and the operational support provided by Europol remain indispensable in complex cross-border investigations. The European Judicial Network continues to facilitate practical cooperation and legal communication between national authorities. The new framework therefore operates alongside existing structures rather than superseding them. This layered approach reflects the complexity of contemporary judicial cooperation and acknowledges that no single instrument is capable of addressing all challenges associated with transnational criminality.

From a broader institutional perspective, the relationship between e-Evidence, Eurojust, Europol, and the European Judicial Network illustrates the gradual evolution of European criminal justice towards a *more* integrated and interconnected system. Each mechanism addresses different dimensions of cross-border cooperation: e-Evidence facilitates access to electronic data, Eurojust supports judicial coordination, Europol

---

[33] AMBOS, *c. d.*, p. 569 et seq.; BÖSE (ed.), *c. d.*, p. 1039 et seq.; HECKER, *Europäisches Strafrecht*, p. 169 et seq.

[34] BÖSE (ed.), *c. d.*, p. 1093 et seq.; HECKER, *Europäisches Strafrecht*, p. 174 et seq.

enhances operational cooperation and intelligence exchange, while the European Judicial Network promotes practical communication between competent authorities. Together, these instruments contribute to a legal environment in which cooperation increasingly transcends traditional territorial boundaries. Their combined operation demonstrates that the effectiveness of modern criminal justice depends not solely upon individual legal instruments but upon the existence of a coherent institutional framework capable of responding to the realities of digitalisation and cross-border criminality. In addition, the significance of this relationship extends beyond practical considerations. It also reflects the constitutional development of the *Area of Freedom, Security, and Justice* as a legal space founded upon mutual trust, shared values, and coordinated action. The e-Evidence framework constitutes an important addition to this evolving structure, but its success depends substantially upon its interaction with existing institutions and mechanisms. The future development of judicial cooperation in criminal matters is therefore likely to be characterised not by the replacement of traditional forms of cooperation, but by their adaptation and integration within an increasingly sophisticated European system of criminal justice.

## POSSIBLE FUTURE DEVELOPMENTS

The adoption of the e-Evidence framework constitutes a step forward in the evolution of judicial cooperation in criminal matters within the European Union. Nevertheless, it should not be regarded as the final stage in the development of legal mechanisms governing access to electronic evidence. The pace of technological innovation continues to outstrip legislative developments, creating new challenges for both national authorities and European institutions. Advances in cloud computing, artificial intelligence (AI), encrypted communications, decentralised digital infrastructures, and emerging data-storage technologies are likely to introduce legal questions that could not have been fully anticipated during the legislative process leading to the adoption of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544. Consequently, the long--term effectiveness of the e-Evidence framework will depend upon its capacity to adapt to technological and societal developments while maintaining compliance with fundamental rights and constitutional principles.

One of the most significant challenges concerns the increasingly global nature of digital services. Although the e-Evidence framework establishes a comprehensive regime within the European Union, a substantial proportion of relevant electronic data continues to be controlled by service providers operating across multiple jurisdictions, including third countries. This reality may generate conflicts between legal obligations arising under European Union law and those imposed by foreign legal systems. Such conflicts are particularly likely in relation to data protection, privacy requirements, and restrictions on the disclosure of electronic information. While international agreements may mitigate some of these difficulties, the growing interconnectedness of digital infrastructures suggests that cross-border access to electronic evidence will remain a complex issue extending beyond the territorial scope of European Union legislation. Future

legal developments should therefore seek to strengthen international cooperation while preserving the autonomy of the European legal order and ensuring adequate protection of fundamental rights. A further challenge relates to the increasing use of encryption technologies. End-to-end encryption has become a standard feature of many digital communication services and plays an important role in protecting privacy, cybersecurity, and freedom of expression. At the same time, encryption may significantly impede access to electronic evidence required for criminal investigations. The tension between privacy and security is therefore likely to remain one of the most contentious issues in future legal and political debates. Legislative responses should avoid simplistic solutions that undermine digital security in pursuit of investigative objectives. Instead, future developments should seek to identify balanced approaches capable of preserving both effective criminal investigations and the integrity of secure communications systems. Any measures affecting encryption technologies must remain fully compatible with the principles of necessity, proportionality, and respect for fundamental rights. From a procedural perspective, the *practical implementation* of the e-Evidence framework will inevitably reveal areas requiring clarification or refinement. Questions concerning judicial oversight, legal remedies, notification obligations, and the protection of affected persons may give rise to divergent interpretations among member states. Such divergences could undermine the uniform application of the framework and weaken mutual trust between national authorities. In order to minimise these risks, greater emphasis should be placed upon the development of common interpretative standards, judicial dialogue, and institutional guidance. The gradual emergence of judicial practice may therefore prove as significant as the legislative framework itself in shaping the future operation of the system.

Several considerations *may* be advanced on the basis of the foregoing analysis. First, future reforms should strengthen procedural safeguards applicable to requests involving particularly sensitive categories of electronic data. Enhanced judicial scrutiny may be justified where investigative measures substantially interfere with privacy, confidentiality of communications, or professional secrecy. Second, consideration should be given to improving transparency mechanisms for individuals whose data has been obtained through cross-border procedures, subject to legitimate investigative interests. Third, greater harmonisation of procedural standards among member states could contribute to legal certainty and reinforce mutual trust within the *Area of Freedom, Security, and Justice*. Finally, future legislative initiatives should be accompanied by regular evaluations assessing both their effectiveness and their impact upon fundamental rights. Such evaluations would facilitate evidence-based policymaking and enable the European Union to respond more effectively to technological and legal developments.

The future evolution of the e-Evidence framework is also likely to be influenced by broader trends affecting European criminal justice. The increasing digitalisation of criminal proceedings, the development of interoperable information systems, the growing role of artificial intelligence in investigative activities, and the expansion of transnational forms of cooperation all suggest that the traditional distinction between domestic and cross-border investigations may gradually become less pronounced. As digital information becomes increasingly central to criminal proceedings, legal systems may

be required to reconsider procedural concepts developed in a predominantly territorial environment. The e-Evidence framework may therefore represent not merely a specific legislative response to practical difficulties but also an indication of a broader transformation affecting the structure of judicial cooperation within the European Union.

Last, but not least, the future success of the e-Evidence system will depend upon its ability to maintain an appropriate balance between effectiveness and legitimacy. Efficient access to electronic evidence is indispensable for combating contemporary forms of criminality, yet effectiveness alone cannot serve as the sole measure of success within a legal order founded upon the rule of law and respect for fundamental rights. The continuing challenge for European legislatures and judicial authorities will be to ensure that technological progress enhances rather than diminishes the values underpinning the constitutional framework of the European Union. Future reforms should therefore be guided by a commitment to both effective judicial cooperation and the preservation of the fundamental principles that define the European legal order. In this respect, the evolution of the e-Evidence framework will remain an important indicator of the broader trajectory of European integration in criminal matters.

## CONCLUSION

The digital transformation of contemporary society has fundamentally altered the conditions under which criminal investigations are conducted and evidence is obtained. Electronic data has become an indispensable source of information in criminal proceedings, while the transnational nature of digital communications has exposed the limitations of traditional mechanisms of judicial cooperation. Against this background, the European Union adopted the e-Evidence framework with the objective of facilitating more efficient access to electronic evidence in cross-border cases. The Regulation (EU) 2023/1543 and the Directive (EU) 2023/1544 represent a significant legislative response to the practical challenges created by technological developments and the increasing reliance upon digital information in the investigation and prosecution of criminal offences.

The e-Evidence framework introduces a substantially different model of judicial cooperation from that traditionally associated with mutual legal assistance and, to a lesser extent, mutual recognition. By enabling competent authorities to address legally binding orders directly to service providers established or represented in another member state, the framework reduces procedural barriers that have historically complicated the acquisition of electronic evidence. This development seeks to enhance the effectiveness of criminal investigations and to ensure that judicial authorities are capable of responding adequately to the realities of the digital environment. At the same time, however, the framework raises important constitutional and legal questions concerning the relationship between efficiency, fundamental rights, and member state sovereignty.

The e-Evidence system affects the principle of member state sovereignty, but not in a manner that can be characterised as its simple erosion or elimination. Rather, the framework reflects the continuing transformation of sovereignty within the constitutional

structure of the European Union. Certain traditional manifestations of territorial control are undoubtedly reduced, particularly through the diminished procedural role of the member state in which a service provider is established or represented. Nevertheless, these limitations arise from legal instruments adopted within the framework of European Union law and accepted by the member states through the exercise of their sovereign powers. Consequently, the framework should be understood as an example of the adaptation of sovereignty to the requirements of an integrated legal order rather than as evidence of its disappearance.

The legitimacy of the e-Evidence framework depends upon the existence of effective safeguards protecting fundamental rights. The acquisition of electronic evidence may significantly interfere with privacy, personal data protection, and other rights guaranteed by the Charter of Fundamental Rights of the European Union. The effectiveness of criminal investigations must therefore be balanced against the requirements of proportionality, legal certainty, judicial protection, and respect for the rule of law. In this regard, the practical implementation of the framework and its interpretation by national courts and the Court of Justice of the European Union will be of decisive importance. The future development of judicial practice will determine whether the balance struck by the European legislature can be maintained in a manner consistent with the constitutional values of the European Union.

The relationship between, on the one hand – e-Evidence, and on the other hand – Eurojust, Europol, and the European Judicial Network, further illustrates that the future of judicial cooperation in criminal matters lies not in the replacement of existing mechanisms but in their integration within a more coherent and technologically adapted system. The e-Evidence framework constitutes one element of a broader process of institutional and legal evolution aimed at strengthening the capacity of the European Union and its member states to address increasingly complex forms of cross-border criminality. As digital technologies continue to evolve, additional reforms are likely to become necessary. Future legislative and judicial developments should therefore seek to preserve an appropriate balance between effectiveness, legal certainty, fundamental rights, and the constitutional principles governing the *Area of Freedom, Security, and Justice*.

From a broader theoretical perspective, the e-Evidence framework illustrates that digitalisation is transforming not only the practical methods of obtaining evidence but also the conceptual foundations of judicial cooperation in criminal matters. The gradual shift from territorially oriented mechanisms towards legally regulated forms of direct cross-border cooperation demonstrates that the traditional relationship between sovereignty, territorial jurisdiction, and investigative powers is undergoing significant adaptation within the European Union. This development should not be understood as diminishing the constitutional role of the member states but rather as reflecting the emergence of new forms of cooperative governance capable of responding to the realities of the digital environment. Consequently, the significance of the e-Evidence framework extends beyond its immediate procedural function and contributes to the broader evolution of European criminal justice as an integrated legal system founded upon mutual trust, effective cooperation, and respect for fundamental rights.

The e-Evidence framework constitutes another step forward in the modernisation of European judicial cooperation in criminal matters. It reflects the European Union's effort to reconcile technological realities with the principles of the rule of law and effective criminal justice. Although important legal and practical challenges remain, the framework provides a foundation for the further development of digital judicial cooperation within the European Union. Its long-term significance lies not only in improving access to electronic evidence but also in illustrating how traditional legal concepts, including sovereignty, may be reinterpreted and adapted within an increasingly interconnected European legal space.

doc. JUDr. et PhDr. mult. Libor Klimek, PhD., Dr. h. c.
Faculty of Law, Matej Bel University in Banská Bystrica
Libor.Klimek@umb.sk
ORCID: 0000-0003-3826-475X