Articles

Studia Iuridica Lublinensia vol. 33, 5, 2024
DOI: 10.17951/sil.2024.33.5.69-85

Andor Gál
University of Szeged, Hungary
ORCID: 0000-0003-2554-8622
andor.gal@juris.u-szeged.hu

New Area of Judicial Cooperation on Criminal Matters in the European Union: The Transmission of Electronic Evidence between Member States*

Nowa dziedzina współpracy sądowej w sprawach karnych w Unii Europejskiej. Przesyłanie dowodów elektronicznych pomiędzy państwami członkowskimi

ABSTRACT

The digitalisation of justice aims to facilitate access to justice, improve overall efficiency and ensure the resilience of justice systems in times of crises, such as the COVID-19 pandemic. Regarding criminal proceedings, the need for digitalisation is made even clearer by the modernization of crime, its partial digitalisation and its cross-border nature. It also follows from the international nature of the digitalisation challenges that the need to meet them cannot be reduced to the level of national law enforcement but is also reflected in the framework of criminal cooperation between the Member States of the European Union. In this context, a new challenge for the digitalisation of justice is the exchange of electronic evidence. The European Union has adopted a Regulation on European Production Orders and European Preservation Orders aimed on the exchange electronic evidence between Member States. This Regulation shall be applied from 18 August 2026. The Regulation prescribes that written communication between competent authorities and designated establishments or legal representatives shall be carried out through a secure and reliable decentralised IT system. However, the Regulation does not regulate execution issues related to the transmission of electronic evidence. Thus, there is a risk that the service providers will carry out official requests through insecure communication channels, even though the European Union already has platforms that are suitable for

CORRESPONDENCE ADDRESS: Andor Gál, PhD, Senior Lecturer, University of Szeged, Faculty of Law, Institute of Criminal Law (BTI), H6721 Szeged, Bocskai u. 10-12, Hungary.

* The research was supported by the Digital Society Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development, and Innovation of the University of Szeged. The author is a member of the "Artificial Intelligence and the Legal Order" research group.

the transfer of evidence. The aim of this paper is to present the specifics of the legal and technical platforms already used by the European Union in this field and to be introduced in the future. The article also examines the relevant legal background related to the operation of these platforms.

Keywords: access to criminal justice; digitalisation; electronic evidence; interoperability; transmission

INTRODUCTION

The rise of digitalisation affects all areas of our lives, our socio-economic, private and public legal relations as well. This occurrence does not leave untouched the criminal proceedings, which provide legal space for the enforcement of a state criminal law claim against individuals. From the perspective of criminal prosecution, the challenges of digitalisation are twofold. On the one hand, the innovation of technological solutions cannot be left untapped in the way law enforcement agencies carry out their activities, as they should make criminal proceedings more timely, efficient and cost-effective, and thus improve the rule of law's expectation of access to justice.[1] On the other hand, the modernisation of crime, its partial digitalisation and its cross-border nature are all factors which necessarily call for the renewal of the legal framework and infrastructure of criminal proceedings to meet the needs of information society.[2]

In line with this, some legislative results to digitalise criminal proceedings can already be found in the Hungarian Criminal Procedure Code.[3] However, the challenges detailed above do not know national borders,[4] so the need to meet them cannot be limited to the level of national law enforcement but must be addressed within the framework of criminal cooperation between the Member States of the European Union. Thus, the European Commission has launched the so-called

[1] For example, see B. Elek, *Költség és időtartalékok a büntetőeljárásban*, "Büntetőjogi Szemle" 2015, no. 1–2, p. 10.

[2] According to criminological research findings, macroeconomic and demographic factors are the primary determinants of past and future changes in crime. However, a third factor is the development of technology. These trends have led to the concept of digital crime in the international literature. See J.D.G. Smith, L.B. Moses, J. Chan, *The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach*, "The British Journal of Criminology" 2017, vol. 57(2), pp. 259–260.

[3] For a presentation of all this, see Cs. Herke, *A digitalizáció szerepe a büntetőeljárásban*, [in:] *A bűnügyi tudományok és az informatika*, ed. K. Mezei, Budapest–Pécs 2019, pp. 104–124; R. Bartkó, *Elektronikus kapcsolattartás a büntetőeljárásban*, [in:] *Az elektronikus eljárások joga*, ed. G. Karácsony, Budapest 2018, pp. 73–98.

[4] See K. Aksamitovska, *Digital Evidence in Domestic Core International Crimes Prosecutions*, "Journal of International Criminal Justice" 2021, vol. 19(1), pp. 189–211.

Digital Criminal Justice project, which aims to improve the individuals' access to justice by implementing to national jurisdictions the following principles:

1. Bodies involved in cross-border judicial cooperation must communicate and exchange information securely via digital means – principle of secure communication and principle of confidentiality of personal data in criminal matters.
2. Ensuring interoperability between the IT systems used by law enforcement authorities in the Member States and those used by EU bodies or agencies – principle of interoperability.
3. Stakeholders have to process data effectively and in line with the requirement of quality assurance – principle of quality data processing.
4. Bodies participating in the European digital criminal justice area should be able to interconnect cross-border criminal cases – principle of interconnectivity of criminal cases.
5. Providing necessary digital support to participants involved in the cross-border cooperation – principle of digital infrastructure.[5]

Considering the above-mentioned principles, the European Commission, under the coordination of Eurojust, has envisaged the following infrastructural improvements:

1. Creation of a secure communication channel to allow exchange of messages, information and evidence electronically across borders in a secure way.
2. Creation a communication tool to enable the secure electronic exchange of judicial cooperation requests and mutual recognition/mutual legal assistance forms, information, messages and evidence.
3. Redesign of Eurojust Case Management System (CMS) to allow its proper functioning and to ensure the needs of its users.
4. Setting up a Joint Investigation Teams' (JIT) Collaboration Platform to coordinate JIT operations, allowing easy communication, as well as the electronic sharing of large amounts of information and evidence between JIT partners.
5. Creation of judicial cases cross-check system to be able to search for case-related information and identify links among cases that are being investigated in other Member States or Justice and Home Affairs (JHA) agencies and EU bodies.
6. Creation of a large-file-solution tool to overcome the limited attachment sizes authorised by mail servers and exchange large amounts of information electronically.[6]

[5] One of the results of this, see European Commission: Directorate-General for Justice and Consumers, *Cross-Border Digital Criminal Justice – Final Report*, 2020, https://data.europa.eu/doi/10.2838/118529 (access: 11.12.2024), hereinafter: DCJ Report.

[6] European Union Agency for Criminal Justice Cooperation, *Digital Criminal Justice*, https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice (access: 11.12.2024).

In accordance with these objectives, the European Parliament and the Council adopted a Regulation on the digitalisation of judicial cooperation and access to justice,[7] intended to apply to both civil and criminal proceedings of a cross-border nature within the EU. The Digitalisation Regulation lays down the rules for the use of electronic communication between competent authorities in judicial cooperation procedures in civil, commercial and criminal matters. This Regulation entered into force on 16 January 2024 and shall be applied from 1 May 2025. It supplements horizontally, rather than replaces, existing rules on digital delivery of documents, digital hearings and other uses of information technology (IT) for cross-border judicial cooperation. In principle, Member States' competent judicial or other authorities would be under a duty to use digital channels of communication, whereas for individuals, the use of such channels would be optional.[8] The Regulation requires national authorities to use e-Codex as a secure communication channel. Under the Digitalisation Regulation, e-Codex will be mandatory for the enforcement of the following legal instruments in the area of cooperation in criminal matters: European arrest warrant, orders freezing property or evidence, mutual recognition to financial penalties, mutual recognition to confiscation orders, mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions, mutual recognition to decisions on supervision measures as an alternative to provisional detention, European protection order, European Investigation Order, and mutual recognition of freezing orders and confiscation orders.[9]

These directions for development show that sharing electronic evidence between Member States can be categorised as a special part of digitalisation of criminal cooperation. In my view, the several principles detailed above should be increasingly applied in transmission of electronic evidence. In harmony with this, the European Council pointed out in its conclusions of 18 October 2018 that solutions need to be found to ensure fast and efficient cross-border access to electronic evidence to combat terrorism and other forms of serious and organised crime effectively at the EU and international level. However, according to the European Council, such transfer of evidence can only be successful if the Member States' law enforcement

[7] Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation (OJ EU L 2023/2844, 27.12.2023), hereinafter: the Digitalisation Regulation.

[8] European Commission, *Legislative Train 02.2024 – A New Push for European Democracy: Digitalisation of Judicial Cooperation*, https://www.europarl.europa.eu/legislative-train/carriage/digitalisation-of-judicial-cooperation/report?sid=7801 (access: 11.12.2024).

[9] Annex II (1) to (11) of the Digitalisation Regulation.

authorities, Europol and Eurojust have the adequate resources needed, as this is the only way to address the security threats arising from technological developments.

Recognising these requirements, the European Parliament and the Council adopted two legislative acts on 12 July 2023 to enhance the cross-border collection of electronic evidence. These are the Regulation (EU) 2023/1543 on European Production Order and European Preservation Order for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings,[10] and 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.[11] The EPO Regulation entered into force on 17 August 2023 and shall be applied from 18 August 2026, and the Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the above-mentioned Directive by 18 February 2026.

It should be noted that until the mandatory application of the EPO Regulation, electronic evidence held by authorities in other Member States could be also obtained by issuing a European Investigation Order (EIO). An EIO is a judicial decision to have specific investigative measures carried out in another Member State with the objective to obtain evidence.[12] As noted in the legal literature by S. Tosza, the EIO may serve to acquire electronic evidence, but it is claimed that its deadlines are too long and create risk that data disappears or is altered in the meantime.[13] In addition, the enforcement of EIO is affected by the principle of territoriality, which can reduce its effectiveness. The creation of European Production Order and European Preservation Order aims to fill these gaps.

As these new types of mutual legal assistance become available, a large increase in the exchange of electronic evidence and data between national authorities is foreseen. Therefore, the EPO Regulation prescribes that written communication between competent authorities and designated establishments or legal representatives shall be carried out through a secure and reliable decentralised IT system.[14] This obligation for competent authorities and service providers to use the decentralised IT system established in for written communication shall apply from one year after the adoption of the implementing acts referred to in Article 25 of the EPO Regulation. These implementing acts shall be adopted by 18 August 2025. Consequently, decentralised IT systems must be in place by the end of August 2026 at the latest.

[10] OJ EU L 191/118, 28.7.2023, hereinafter: the EPO Regulation.

[11] OJ EU L 191/181, 28.7.2023.

[12] S. Tosza, *All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relationship between the European Investigation Order and the European Production Order*, "New Journal of European Criminal Law" 2020, vol. 11(2), p. 164.

[13] *Ibidem*, p. 169.

[14] Article 19 of the EPO Regulation.

In this context, it has to be emphasised that the Digitalisation Regulation does not impose the mandatory use of e-Codex in relation to the legal instruments covered by the EPO Regulation. Thus, in addition to e-Codex, other available platforms (decentralised IT systems) could be used for the exchange of electronic evidence by national authorities.

Information on the establishment of the above-mentioned decentralised IT system is currently unavailable. However, the secure operation of this system has crucial importance, therefore the jurisprudential analysis of the relevant requirements cannot be ignored. Taking all of this into consideration, the present paper examines the issues related to the exchange of electronic evidence between Member States, especially the practicalities of evidence transfer. For this reason, it is not my aim to analyse the procedural and, above all, jurisdictional dilemmas raised by the adopted regulation, as they require separate academic examination, and there are already examples of this approach in the legal literature.[15]

RESEARCH METHODS

The paper focuses on practical issues concerning the transmission of electronic evidence between national authorities. On this basis, the article outlines some of the possibilities for exchanging electronically available data and analyses them from an information and data security perspective. It is necessary to recall here that cybersecurity focuses on managing the risks that endanger the proper, safe, performant and qualitative functioning of the technology.[16] It has a direct approach on the cause effect phenomena and seeks to solve problems that have implications into all aspects of human life.[17] It has to be stressed, that both the infrastructural and the legal background for this specific segment of cooperation between EU Member States is currently being developed. For this reason, the information security or cybersecurity focus permeates the presentation of data transfer channels and the analysis of the relevant legislative acts.

[15] As an example, see S. Tosza, *op. cit.*, pp. 161–183; K. Karsai, *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, "Hungarian Journal of Legal Studies" 2019, vol. 60(2), pp. 155–172.

[16] This topic was examined from a similar perspective in the German literature. See D. Brodowski, *Die Digitalisierung der strafjustiziellen Zusammenarbeit in der EU*, "Zeitschrift für die gesamte Strafrechtswissenschaft" 2023, vol. 135(3), pp. 659–678.

[17] E.F. Popescu, *Complementary Cybersecurity*, "International Journal of Information Security and Cybercrime" 2020, vol. 9(2), p. 33.

RESEARCH AND RESULTS

1. The role of technological innovations in the functioning of national authorities

In the operation of law enforcement agencies, technological innovations can play administrative-organisational-coordinative as well as decision-supportive role. Solutions connected to the former category are aimed at improving administrative aspects of law enforcement tasks. The second category includes all activities that aimed at prevention and detection of criminal offences.[18] It is not possible to provide a full list of digital tools used in decision-supportive role in criminal proceedings. The main areas of them can be identified as follows: predicting the commission of crimes, automating the detection of crimes and their perpetrators, and automation of decision-making processes and automated analysis of evidence.[19]

The use of technological innovations for administrative activities has led to a variety of communication method, such as remote communication between authorities (e.g. videoconferencing), ensuring the electronic forwarding of documents issued and processed by the authorities (e.g. electronic document management) or introducing tools to automate certain law enforcement activities (e.g. the preparation of requests or the reporting of criminal offences). The transmission of electronic evidence can also be included in the administrative activities of authorities.

Legal document automation software available on the technology market can be easily used in the administrative work of services, as it is capable of quickly preparing standard document elements.[20] Similarly, the work of law enforcement agencies can be facilitated by the proliferation of automatic speech recognition (ASR) and optical character recognition (OCR) systems, which can significantly speed up formal activities (e.g. recording a witness statement).[21] The use of artificial intelligence can also be used in this area. For instance, some investigative authorities are already supported by chatbots that allow the immediate reporting

[18] M. Dymitruk, *Legal Tech in the Law Enforcement Agencies*, [in:] *Legal Tech: Information Technology Tools in the Administration of Justice*, eds. D. Szostek, M. Zalucki, Baden-Baden 2022, pp. 259–261.

[19] *Ibidem*, p. 262.

[20] Automatic document assembly software is essentially a combination of text templates and algorithms (coded rules containing conditional relations). These tools are part of the second generation of technological innovations in the field of justice, and the legal profession has been rapidly started to use them early on. See M. Laurintsen, *Document Automation*, [in:] *Legal Informatics*, eds. D.M. Katz, R. Dolin, M.J. Bommarito, Cambridge 2021, pp. 69–72; J. Kery-Tyerman, A.J. Shankar, *The Core Concepts of E-Discovery*, [in:] *Legal Informatics…*, pp. 311–312.

[21] M.J. Bommarito, *Preprocessing Data*, [in:] *Legal Informatics…*, pp. 58–60.

of criminal offences. Artificial intelligence may also help in organising and linking electronic evidence to cases.

In the field of administrative activities, the use of technological tools is essentially aimed at streamlining and speeding up the processing of cases. The use of digitalisation in this area, while important for the functioning of certain type of services, does not in itself revolutionise the way in which law enforcement agencies perform their tasks, and does not in itself make the operation of the judiciary different, from an IT point of view. In terms of judicial cooperation, real progress can be achieved if the use of digital tools is integrated into substantive law enforcement tasks. The latter area primarily concerns the functioning of the bodies coordinating cooperation in criminal matters between Member States. The key measure of the effectiveness of communication between these authorities is the criterion of interoperability.

2. Basic requirement of an efficient operation: interoperability

According to the opinion of the European Interoperability Framework,[22] "interoperability is the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems".[23]

Technological interoperability includes applications and infrastructures linking systems and services. A technological interoperability platform allows two organizations to reliably exchange messages, but the actual understanding of message content remains outside its scope.[24]

"Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'."[25] This implies that, despite divergences in the structure, organisation and content of the exchanged

[22] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework – Implementation Strategy, Brussels, 23.3.2017, COM(2017) 134 final. European Interoperability Framework is a commonly agreed approach to the delivery of European public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models and recommendations.

[23] European Commission, *New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations*, 2017, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (access: 11.12.2024), p. 5.

[24] N. Carboni, M. Velicogna, *Electronic Data Exchange within European Justice: e-Codex Challenges, Threats and Opportunities*, "International Journal for Court Administration" 2012, vol. 4(3), p. 107.

[25] European Commission, *New European Interoperability Framework…*, p. 29.

data, the intended meaning is correctly conveyed, the information is correctly acquired and the expected actions are understood and undertaken.[26]

Organisational interoperability "refers to the way in which public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals".[27]

Legal interoperability is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This category can also be defined a functional environment in which users may legally access and use the data of others without seeking permission on a case-by-case basis.[28]

The system used for the exchange of electronic evidence must have all the above-mentioned characteristics of interoperability. The legal basis for the exchange of electronic evidence is already given, as the EPO Regulation explicitly provides for the use of a decentralised IT system for national authorities. Making the use of a decentralised IT system compulsory under EU law makes the requirement for legal interoperability feasible. In my view, the additional requirements related to interoperability can only be understood by describing the characteristics of the concrete platform.

3. Available platforms for the transmission of electronic evidence in the European Union

3.1. E-Codex

E-Codex (e-Justice Communication via Online Data Exchange) is essentially a package of different software components that allows users – competent judicial authorities, practitioners and citizens – to manage documents, legal forms, evidence and other information quickly and securely by electronic means. In this way, e-Codex provides an information technology support for civil and criminal matters, an interoperable, secure and decentralised communication network linking national IT systems. The system is legally defined in Article 3 (1) of Regulation (EU) 2022/850[29] as a "decentralised and interoperable system for cross-border communication for the purpose of facilitating the electronic exchange of data, which includes any content transmissible in electronic form, in a swift, secure and reliable manner in the area of judicial cooperation in civil and criminal matters".

[26] N. Carboni, M. Velicogna, *op. cit.*, p. 107.

[27] European Commission, *New European Interoperability Framework…*, p. 28.

[28] N. Carboni, M. Velicogna, *op. cit.*, p. 106.

[29] Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ EU L 150/1, 1.6.2022), hereinafter: the e-Codex Regulation.

The technical architecture of the e-Codex system is illustrated in Figure 1.

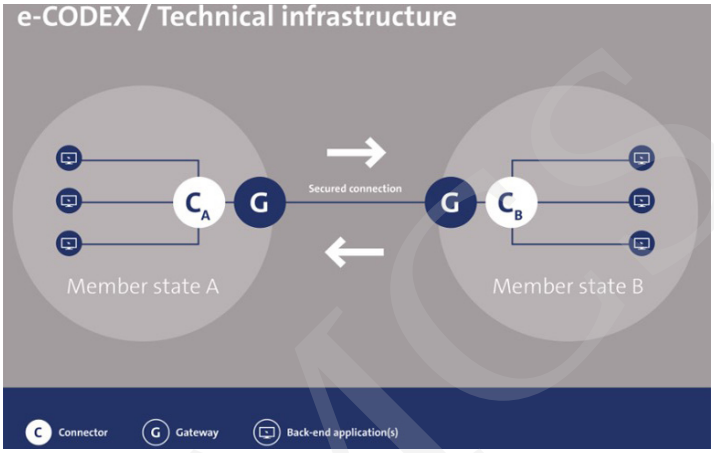

Figure 1. The technical architecture of the e-Codex system

Source: https://www.e-codex.eu/tech (access: 12.3.2024).

The e-Codex Regulation itself does not impose any obligation to use the system actively or passively, but merely creates the legal framework for the technical infrastructure. However, in its communication entitled "Digitalisation of justice in the European Union – A toolbox of opportunities", the Commission identified e-Codex as the main tool for creating a communication network between national IT systems.[30] The Digitalisation Regulation also refers to e-Codex as the main decentralised IT platform for data exchange between national authorities.

The e-Codex Regulation stipulates that only authorized access points may be connected to the system. These may be operated by institutions, bodies, offices and agencies of the Union and in the Member States by public authorities, but also by duly authorized legal persons and legal organizations (Article 3 (4) of the e-Codex Regulation). The e-Codex system is then intended to facilitate communication between these access points and via them into the respective IT systems.[31]

One of the key concepts adopted by e-Codex to achieve such simplification is the creation of a "circle of trust" between the judicial authorities involved. The idea of "circle of trust" should provide the basis for the judicial authorities to trust the information provided through e-Codex. In other words, e-Codex works on each

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitalisation of justice in the European Union – A toolbox of opportunities, Brussels, 2.12.2020, COM/2020/710 final.

[31] D. Brodowski, *op. cit.*, p. 661.

Member State's trust of other Member States on issues such as confidentiality, e-Identification, e-Signature, e-Documents, e-Payment and transport.[32]

The e-Codex system did not initially benefit from the electronic identification and trust services provided by the eIDAS Regulation[33] as the infrastructure predates this Regulation. This meant that an e-Identification and e-Signature had to be developed for e-Codex as they were both a technical and legal problem.[34]

However, in Hungary, the e-Codex system is not yet used by the criminal courts at all, and the Hungarian courts communicate with other EU Member States' authorities by e-mail. Thus, as E.A. Ontanu has already stated, "for e-Codex to function as the system facilitating cross-border electronic communication, national IT systems will have to become technically interconnectable with the EU decentralised system, or, alternatively, Member States can choose to rely on the Reference Implementation Software solutions".[35] The system will have to be created and managed by the European Commission for Member States to use, if they choose this solution.

3.2. E-EDES

The e-Evidence Digital Exchange System (e-EDES) is an IT tool that allows Member States' authorities to securely exchange European investigation orders, mutual legal assistance requests and electronic evidence in digital form.

At present, the authorities use postal or electronic methods, which are considered outdated, slow and lacking in security standards. Therefore, the aim of creating e-EDES was to guarantee the security of the exchange of these types of data and to increase the efficiency and speed of existing cooperation procedures, while allowing the authenticity and integrity of the documents transmitted to be checked. Its development will at the same time interoperability with national case management systems.

Member State experts involved in the development of e-EDES have called for a strongly decentralised architecture for the system, which means that it will require a secure portal in each Member State, accessible in national language. The DCJ Report explicitly mentions e-EDES for the transmission of specific documents, in particular electronic evidence, between national authorities. European Commission has tailored this tool to the needs of the European criminal justice area: e-EDES is

[32] N. Carboni, M. Velicogna, *op. cit.*, p. 113.

[33] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257/73, 28.8.2014).

[34] E.A. Ontanu, *The Digitalisation of European Union Procedures: A New Impetus Following a Time of Prolonged Crisis*, "Law, Technology and Humans" 2023, vol. 5(1), p. 104.

[35] *Ibidem*, p. 99.

based on common open standards and open-source implementations (e.g. e-Codex connector and Domibus Gateway).

However, e-EDES needs further development, which is currently being carried out in the framework of the EXEC II project.[36] The EXEC II goes beyond the initial digitalisation efforts and gives project partners the opportunity to integrate the e-EDES environment into their national solutions. Indeed, the purpose of using this platform is twofold. Firstly, it is possible to integrate the e-EDES environment into national case management systems for data exchange. Secondly, it is also true that project partners can integrate their national authentication solutions into e-EDES, avoiding redundant and error-prone user administration, while at the same time enhancing the usability of the platform by re-using existing user data.

The EXEC II project also aims:

- to integrate national case management systems into the e-EDES platform;
- to enable the reuse of stored data for both the national register and e-EDES;
- to enable instant communication between stakeholders (similar to the Europol SIENA application);
- to give Eurojust direct access to e-EDES, initially only through the national correspondents;
- the management of electronic signatures;
- development of an artificial intelligence-based module capable of machine translation.[37]

In addition, future development plans include the inclusion of the EJN Atlas tool in e-EDES, which will allow representatives of e-EDES partner bodies to find the competent authority in another Member State in a user-friendly way.

In Hungary, according to the order of the Prosecutor General, e-EDES shall be used by the Prosecutor's Office to send European Investigation Orders and mutual legal assistance requests as issuing authorities to authorities of the Member States of the European Union and to receive them as executing authorities from authorities of the Member States of the European Union that have joined the System.[38] Unfortunately, the connection of the Hungarian courts' organisation to the decentralised IT system has not yet been solved in the case of e-EDES.

[36] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitalisation of justice in the European Union – A toolbox of opportunities, Brussels, 2.12.2020, COM/2020/710 final.

[37] DCJ Report, p. 102.

[38] Order No. 5/2023 of the Prosecutor General of Hungary.

3.3. Eurojust Case Management System

Member States are obliged to provide the European Union's Agency for Judicial Cooperation in Criminal Matters (Eurojust) with all the information it needs to carry out its task of facilitating judicial cooperation and coordination. The fulfilment of these obligations is a challenge for Member States, as the digital platform used by Eurojust is very outdated.

In this context, the redesign of Eurojust's Case Management System (CMS) within the Digital Criminal Justice project is a key element of the IT modernisation of cross-border digital criminal justice. According to the preliminary plans, the main components of the new database to be developed by Eurojust would be the Core CMS, the Counter Terrorism Register, the JIT Admin Portal, the Action Day Collaboration Platform and the Integration Layer.[39]

The Core CMS component, as part of the redesigned Eurojust CMS, is the main operational system supporting the day-to-day activities of the Eurojust national offices, i.e. the registration, management and recording of all cases of cross-border judicial cooperation supported by Eurojust.

Council Decision 2005/671/JHA48[40] requires Member States to provide Eurojust with information on terrorist offences. To this end, the Counter-Terrorism Register was launched in 2019 to help prosecutors to coordinate more actively and to identify perpetrators or networks under investigation in different countries. However, this platform currently has limited functionalities which requires extensive manual intervention.[41]

The Action Day Collaboration Platform would provide digital support for collaborations that do not yet constitute a joint investigation team (JIT) but require active and regular cooperation between Member States' bodies. JITs can operate from a few months to a few years, whereas Action Day collaboration can last up to a few months. Another important difference is that the day of action cooperation is coordinated by Eurojust, however a joint investigation team can be set up without Eurojust's involvement. On this basis, electronic system supporting day-to-day cooperation has to be integrated into the Eurojust CMS with due regard to the fact that EU law now provides for the optional use of a separate platform for communication between members of a joint investigation team.[42]

---

[39] DCJ Report, p. 116.

[40] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ EU L 253/22, 29.9.2005).

[41] DCJ Report, p. 120.

[42] See Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726 (OJ EU L 132/1, 17.5.2023).

CONCLUSIONS

The perpetrators of cross-border organised crime use the most modern telecommunication tools to carry out their activities. In order to increase the effectiveness of the fight against these crimes, law enforcement agencies must get a step ahead in the use of modern technologies. In comparison, the predominance of paper-based administration for handling of cross-border criminal cases remains unchanged. Therefore, it is precisely essential to speed up the transition to digital administration in EU legal proceedings.

This is particularly true for the exchange of evidence stored in electronic form, as this form of cooperation between national authorities is a key element of a successful criminal procedure. With these modernisation requirements in mind, the EU has also recognised the benefits of digitalisation in the field of judicial cooperation in criminal matters. This has led to a rapid development of both the legal and infrastructural background, which have been presented in this paper.

As I have discussed in detail in the article, the European Union has set the objective of creating a digital area of justice. This includes the simultaneous development of a number of secure data transmission platforms that will enable Member States and EU law enforcement agencies to communicate faster, more efficiently and more securely from a law enforcement and data protection perspective.

As I have pointed out above, the European Union envisages e-Codex, e-EDES and Eurojust's modernised CMS as the main digital communication channels for criminal matters within the area of freedom, security and justice. The task for the near future will be to make these systems interoperable with each other, with other EU databases (e.g. VOCU,[43] SIENA,[44] JIT online platform, etc.) and with national registers.

It has to be stressed that the exercise of the right of access to case-related documents should also be ensured for electronic evidence. However, it is not clear whether the available evidence transfer platforms can provide access to clients in order to exercise their right to inspection of documents (case files) or not.

In summary, I believe that the platforms presented may be suitable for data transmission that meets the requirements cited above. In my view, the exchange of electronic evidence should also take place within these platforms. As described in this paper, the e-EDES database seems to be the most appropriate tool for this purpose. However, as can be seen from the Hungarian example mentioned above,

[43] The Virtual Operations Coordination Unit is an IT application and registration system developed by OLAF under the Anti-Fraud Information System (AFIS), which facilitates the exchange of operational law enforcement information between the competent authorities of the Member States and OLAF.

[44] The Secure Information Exchange Network Application is a state-of-the-art platform used by Europol to enable the rapid and user-friendly exchange of law enforcement data between Europol liaison officers, Member States' investigative authorities and third parties with which Europol has concluded cooperation agreements.

the connection of Hungarian courts to e-Codex and e-EDES is not yet solved. As long as this technological interoperability requirement is not fulfilled, mandatory electronic communication between public authorities cannot be imposed.

REFERENCES

Literature

Aksamitovska K., *Digital Evidence in Domestic Core International Crimes Prosecutions*, "Journal of International Criminal Justice" 2021, vol. 19(1), **DOI: https://doi.org/10.1093/jicj/mqab035**.

Bartkó R., *Elektronikus kapcsolattartás a büntetőeljárásban*, [in:] *Az elektronikus eljárások joga*, ed. G. Karácsony, Budapest 2018.

Bommarito M.J., *Preprocessing Data*, [in:] *Legal Informatics*, eds. D.M. Katz, R. Dolin, M.J. Bommarito, Cambridge 2021.

Brodowski D., *Die Digitalisierung der strafjustiziellen Zusammenarbeit in der EU*, "Zeitschrift für die gesamte Strafrechtswissenschaft" 2023, vol. 135(3), **DOI: https://doi.org/10.1515/zstw-2023-0026**.

Carboni N., Velicogna M., *Electronic Data Exchange within European Justice: e-Codex Challenges, Threats and Opportunities*, "International Journal for Court Administration" 2012, vol. 4(3).

Dymitruk M., *Legal Tech in the Law Enforcement Agencies*, [in:] *Legal Tech: Information Technology Tools in the Administration of Justice*, eds. D. Szostek, M. Zalucki, Baden-Baden 2022.

Elek B., *Költség és időtartalékok a büntetőeljárásban*, "Büntetőjogi Szemle" 2015, no. 1–2.

Herke Cs., *A digitalizáció szerepe a büntetőeljárásban*, [in:] *A bűnügyi tudományok és az informatika*, ed. K. Mezei, Budapest–Pécs 2019.

Karsai K., *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, "Hungarian Journal of Legal Studies" 2019, vol. 60(2), **DOI: https://doi.org/10.1556/2052.2019.00010**.

Kery-Tyerman J., Shankar A.J., *The Core Concepts of E-Discovery*, [in:] *Legal Informatics*, eds. D.M. Katz, R. Dolin, M.J. Bommarito, Cambridge 2021.

Laurintsen M., *Document Automation*, [in:] *Legal Informatics*, eds. D.M. Katz, R. Dolin, M.J. Bommarito, Cambridge 2021.

Ontanu E.A., *The Digitalisation of European Union Procedures: A New Impetus Following a Time of Prolonged Crisis*, "Law, Technology and Humans" 2023, vol. 5(1).

Popescu E.F., *Complementary Cybersecurity*, "International Journal of Information Security and Cybercrime" 2020, vol. 9(2).

Smith J.D.G., Moses L.B., Chan J., *The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach*, "The British Journal of Criminology" 2017, vol. 57(2), DOI: https://doi.org/10.1093/bjc/azw096.

Tosza S., *All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relationship between the European Investigation Order and the European Production Order*, "New Journal of European Criminal Law" 2020, vol. 11(2), **DOI: https://doi.org/10.1177/2032284420919802**.

Online sources

European Commission, *Legislative Train 02.2024 – A New Push for European Democracy: Digitalisation of Judicial Cooperation*, https://www.europarl.europa.eu/legislative-train/carriage/digitalisation-of-judicial-cooperation/report?sid=7801 (access: 11.12.2024).

European Commission, *New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations*, 2017, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf (access: 11.12.2024).

Reports

European Commission: Directorate-General for Justice and Consumers, *Cross-Border Digital Criminal Justice – Final Report*, 2020, https://data.europa.eu/doi/10.2838/118529 (access: 11.12.2024).

European Union Agency for Criminal Justice Cooperation, *Digital Criminal Justice*, https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice (access: 11.12.2024).

Legal acts

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework – Implementation Strategy, Brussels, 23.3.2017, COM(2017) 134 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitalisation of justice in the European Union – A toolbox of opportunities, Brussels, 2.12.2020, COM/2020/710 final.

Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences (OJ EU L 253/22, 29.9.2005).

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 (OJ EU L 191/181, 28.7.2023).

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257/73, 28.8.2014).

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ EU L 150/1, 1.6.2022).

Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726 (OJ EU L 132/1, 17.5.2023).

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ EU L 191/118, 28.7.2023).

Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation (OJ EU L 2023/2844, 27.12.2023).

ABSTRAKT

Cyfryzacja wymiaru sprawiedliwości ma na celu ułatwienie dostępu do wymiaru sprawiedliwości, poprawę ogólnej efektywności oraz zapewnienie odporności systemów wymiaru sprawiedliwości w okresach kryzysowych, jak np. pandemia COVID-19. W przypadku postępowania karnego potrzebę cyfryzacji widać jeszcze wyraźniej ze względu na modernizację przestępczości, jej częściową cyfryzację oraz transgraniczny charakter. Z międzynarodowego charakteru wyzwań związanych z cyfryzacją wynika też to, że konieczność sprostania im nie może zostać ograniczona do poziomu krajowych organów ścigania, lecz znajduje odzwierciedlenie także w ramach współpracy karnej między państwami członkowskimi Unii Europejskiej. Wobec tego nowym wyzwaniem dla cyfryzacji wymiaru sprawiedliwości jest przekazywanie dowodów elektronicznych. Unia Europejska przyjęła rozporządzenie w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dotyczące przekazywania dowodów elektronicznych pomiędzy państwami członkowskimi. Rozporządzenie to będzie stosowane od 18 sierpnia 2026 r. Rozporządzenie przewiduje, że komunikacja pisemna między właściwymi organami lub między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi powinna być prowadzona za pośrednictwem bezpiecznego i niezawodnego zdecentralizowanego systemu teleinformatycznego. Rozporządzenie nie reguluje jednak kwestii wykonawczych związanych z przesyłaniem dowodów elektronicznych. Istnieje zatem ryzyko, że usługodawcy będą realizować oficjalne wnioski za pośrednictwem niepewnych kanałów komunikacyjnych, nawet jeśli Unia Europejska dysponuje już platformami, które są odpowiednie do przekazywania dowodów. Celem opracowania jest przedstawienie specyfiki platform prawno-technicznych wykorzystywanych już przez Unię Europejską w tej dziedzinie oraz ich wprowadzenie w przyszłości. W artykule przeanalizowano również odpowiednie tło prawne związane z działaniem tych platform.

Słowa kluczowe: dostęp do karnego wymiaru sprawiedliwości; cyfryzacja; dowody elektroniczne; interoperacyjność; przesyłanie