Articles

Studia Iuridica Lublinensia vol. 33, 5, 2024
DOI: 10.17951/sil.2024.33.5.125-153

Hanna Kuczyńska
Polish Academy of Sciences, Poland
ORCID: 0000-0002-1446-2244
hkuczynska@gmail.com

The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change

Pakiet e-dowodów w prawie Unii Europejskiej z perspektywy polskiej. Najwyższy czas na systemową zmianę

ABSTRACT

The article focuses on the problems resulting from the adoption of Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Once the Regulation enters into force (18 August 2026), national courts will be able to include data obtained as a result of issuing of a European Production Order and (at an earlier stage) a European Preservation Order in the case file and then assess their admissibility. The e-evidence package offers procedural authorities a tool to gather electronic evidence. At the same time, this package is silent about the way these evidence – so easily and quickly acquired from service providers in other Member States – should be treated by national courts. Meanwhile, this is the stage that is decisive for justice systems and may lead to numerous – both legal and practical – problems. Therefore, the article deals with the problem of how the e-evidence package looks from the Polish perspective and how Polish courts can admit electronic evidence into criminal trial. Furthermore, attention is drawn to the problem of direct application of this Regulation and the problem of equivalence of the powers of national authorities towards service providers residing in other states and service providers residing in Poland. In this area, an analysis of national legal framework is presented, the aim of which is to show whether there are currently adequate and equivalent legal grounds for issuing production and preservation orders in national law towards national providers. The analysis shows that several changes in the Polish law are necessary in order to secure and ensure the effective application of the Regulation.

Keywords: criminal trial; electronic evidence; European Production Order; admissibility of evidence; the EU cooperation in criminal matters

CORRESPONDENCE ADDRESS: Hanna Kuczyńska, PhD, Prof. Dr. Habil., Full Professor, Polish Academy of Sciences, Institute of Law Studies, Pałac Staszica, Nowy Świat 72, 00-330 Warszawa, Poland.

INTRODUCTION

On 12 July 2023, after five years of negotiations,[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings[2] was finally adopted. The Regulation forms an element of the e-evidence package, which consists of a European Production Order (EPO), that allows a judicial authority in one Member State to obtain electronic evidence (such as e-mails, IP addresses, texts or messages in applications, as well as any information necessary to identify a perpetrator) directly from a service provider or its legal representative in another Member State; once providers receive an EPO from another state's judicial authority, they are obliged to respond – under the threat of a sanction (in the form of pecuniary penalties, which are set in national law of the Member States – with the limit resulting from Article 15 (1) of the Regulation). The second element of this package is a European Preservation Order (EPrO), that will allow a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data (via a European Investigation Order or an EPO). The Regulation shall apply from 18 August 2026, which gives Members States and service providers three years to prepare the operational framework in order to comply with the new obligations. There is also an accompanying piece of legislation that is the 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.[3] Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 18 February 2026.

This text focuses on the problems that arise when national courts need to include data obtained as a result of issuing of an EPO and (at an earlier stage) an EPrO in the case file and then assess their admissibility.[4] The e-evidence package offers to

---

[1] About the history of negotiations, see S. Tosza, *The E-evidence Package Is Adopted: End of a Saga or Beginning of a New One?*, "European Data Protection Law Review" 2023, vol. 9(2), p. 163; G. Forlani, *The E-evidence Package: The Happy Ending of a Long Negotiation Saga*, "Eucrim" 2023, no. 3, pp. 174–181; M. Kusak, *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, "Gdańskie Studia Prawnicze" 2024, no. 2, p. 82; idem, *Mutual Trust to Obtain Evidence in the EU: Is the Bar Law or High?*, [in:] *Current Issues of EU Criminal Law*, eds. A. Ochnio, H. Kuczyńska, Warszawa 2022, pp. 73–88.

[2] OJ EU L 191/118, 28.7.2023.

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

[4] On the example of Germany, see K. Pfeffer, *Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln*, "Eucrim" 2023, no. 3, pp. 170–171.

the procedural authorities the tool to gather electronic evidence. As it is advertised by the EU Commission, "the e-evidence package will make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals".[5] At the same time, this package is silent about the way these evidence – so easily and quickly acquired from service providers in other Member States – are treated by national courts. Meanwhile, this is the stage that is decisive for justice systems and may lead to numerous – both legal and practical – problems. Therefore, the paper deals with the problem of how the e-evidence package looks from the Polish perspective and how Polish courts can admit electronic evidence into criminal trial. Furthermore, attention is drawn to the problem of direct application of Regulation 2023/1543 and the problem of equivalence of the powers of national authorities towards service providers residing in other states and service providers residing in Poland. In this area, an analysis of national legal framework is presented, the aim of which is to show whether there are presently legal grounds for issuing production and preservation orders in national law towards national providers. As a result of the conducted analysis, the author emphasizes that several changes in the Polish law are necessary in order to secure and ensure the effective application of the Regulation.

The next group of problems arise from the fact that Regulation 2023/1543 bases on a model of direct cooperation while excluding the need to contact judicial organs in the Member State of the provider. It shortens the way between the electronically stored data (in possession of the service provider) in another Member State and the issuing judicial organ. Therefore, it is hardly "mutual cooperation" in criminal matters anymore, since the judicial organ for the first time is competent to reach a private entity in another Member State: it is a "privatization of the mutual cooperation model".[6] In consequence, it is rather a tool to avoid cooperation with other Member States' judicial authorities. The Regulation departs from the existing models of judicial co-operation and mutual recognition in EU law, which are based on cooperation and communication between public authorities in Member States.

In consequence, with the direct route from the provider to the issuing state's courtroom, the only guarantor of compliance with fundamental rights and procedural guarantees is the court which adjudicates the case where the e-evidence obtained as a result of issuing an EPO is used. Even the grounds for refusal are

[5] See European Commission, *E-evidence – Cross-Border Access to Electronic Evidence*, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (access: 14.12.2024).

[6] V. Mitsilegas, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), pp. 263–265. See also Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM(2018) 225 final.

assessed by a non-judicial organ – the service provider. There is only a notification procedure possible (to executing Member States' judicial authorities) provided in the Regulation, according to which, if the order concerns traffic or content data, a notification to the enforcing authority shall be sent simultaneously with the certificate addressed to the service provider. Its effect is however limited by the rule excluding from this obligation the category of national cases (Article 8 (2) of the Regulation).[7] Therefore, the role of the adjudicating court as the guarantor of application of the conditions regulated in the Regulation and procedural rights of the accused is crucial and has to be analysed.

The final group of problems taken into consideration relates to the scope of Regulation 2023/1543. The Regulation presents a definition of "electronic evidence"; therefore, it is possible to distinguish "electronic evidence" from "digital evidence". According to Article 3 (8) of the Regulation "electronic evidence" means subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form, at the time of the receipt of a European Production Order Certificate or of a European Preservation Order Certificate. Electronic evidence are data that are: stored in an electronic form either by the service provider or on its behalf; stored at the time of receipt of the EPO or EPrO – the order concerns only the data already in the possession of the service provider and not any data to be obtained in the future, thus excluding any future surveillance. The order may relate to three types of data: subscriber data, traffic data or content data.[8] All the other evidence of digital character not falling into the scope of "electronic evidence" as provided in the Regulation, should be defined as a wider group of digital evidence.

Therefore it would be possible to claim that "electronic evidence" is evidence coming directly from the service provider, whereas "digital evidence" is evidence of digital character from other sources, such as Internet open sources, social media, satellites, drones, CCTV.[9] The Regulation provides thus the first in the Polish law definition of electronic evidence – on the EU level – stating what they are and how

[7] More on this topic, see S. Tosza, *The E-evidence Package…*, p. 168.

[8] Idem, *The European Commission's Proposal on Cross-Border Access to E-Evidence*, "Eucrim" 2018, no. 4; idem, *W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, pp. 48–52.

[9] So far, the two notions were understood identically and the two words were used alternately. According to P. Lewulis (*Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, vol. 33, p. 43), the definition of "digital evidence" is broad and includes all the evidentiary value information drawn from openly accessible online data. All general considerations on digital evidence use in Polish criminal proceedings apply to either covert and open-source data unless stated otherwise. According to A. Lach (*Dowody elektroniczne w procesie karnym*, Toruń 2004, pp. 28–30), electronic evidence is computer-generated evidence. These are evidence in the creation of which a computer participated, information transmitted or encoded in a binary form that may be important in court proceedings.

they should be gathered, according to what standards and what guarantees should be protected. It has to be though analysed whether the equivalent provisions may be applied in case of gathering and assessing admissibility of electronic evidence and digital evidence.

It is also important to underline that EPO and EPrO may be issued only in the framework and for the purposes of criminal proceedings (Article 1 of the Regulation). Moreover, the Regulation also applies to proceedings initiated by an issuing authority to locate a convicted person that has absconded from justice, in order to execute a custodial sentence or a detention order following criminal proceedings (with exception of custodial sentences or detention orders imposed by a decision rendered *in absentia*). In consequence, both orders cannot be issued in the scope of operational Police activities, before a criminal investigation has begun. European Production Orders cannot be used as a tool of discovery of crimes, but only as a tool of acquiring evidence of already investigated crimes. The Regulation's Preamble explains this prerequisite even further, stating in Recital 24 that in the framework of criminal proceedings, the European Production Order and the European Preservation Order should only be issued for specific criminal proceedings concerning a specific criminal offence that has already taken place, after an individual evaluation of the necessity and proportionality of those orders in every single case, taking into account the rights of the suspect or the accused person.

PROBLEMS WITH DIRECT APPLICATION OF THE EU REGULATION

The EU legislator decided to regulate the e-evidence package in the form of a regulation in order to place obligations both on judicial authorities and service providers in the area of acquiring electronic evidence in other Members States. According to Article 288 of the consolidated version of the Treaty on the European Union and the Treaty on the Functioning of the European Union[10] (TFEU) a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. The Treaty allows to use this instrument as a tool of regulating the judicial cooperation in criminal matters.[11]

This tool is convenient from the point of view of EU legislator: whereas directives are merely binding as to the result to be achieved upon each Member State and allow for different approaches to implementation in every Member State, provisions of regulations are applicable directly and take precedent over national

[10] OJ C 326/47, 26.10.2012.

[11] See J.P. Mifsud Bonnici, M. Tudorica, J.A. Cannataci, *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, [in:] *Handling and Exchanging Electronic Evidence Across Europe*, eds. M.A. Biasiotti, J.P. Mifsud Bonnici, F. Turchi, Cham 2018, p. 193.

legislation in case the two contradict one another. In case, where there is a need to create identical rights and obligations for individuals and judicial authorities, that will be uniformly applied, it is clear that regulations possess a clear and key advantage over directives.[12] Also, whereas directives have only vertical direct effect, regulations have both horizontal and vertical direct effect – allowing not only individuals to invoke their rights from state authorities but also individuals to bring actions against other individuals based on rights provided in the regulation. Regulations do not require either transposition into the system of internal laws of the Member States or announcements in accordance with the rules of national law.

In the opinion of the Court of Justice, the direct application of a regulation means that its entry into force and application are not dependent on any act incorporating it into national law.[13] Moreover, Member States have no competence to adopt provisions implementing a regulation, changing its scope or supplementing its provisions, unless this is expressly provided for in a regulation.[14] They may not make the application of a regulation subject to any conditions provided for in national law, in particular as regards the rights and obligations of individuals provided for in a regulation. In the judgment of 10 October 1973, the Court stated that the establishment of a national act that repeats the provisions contained in the regulation is *per se* a violation of EU law.[15] Moreover, the transformation of the content of the regulation into national law actually makes the competence of the Court of Justice to declare the regulation invalid or interpret it illusory. In the opinion of the Court of Justice, the ban on transformation is justified not only due to the principle of primacy of EU law but is also necessary to ensure uniform and simultaneous application of EU law throughout the Union.

In consequence, the provisions of Regulation 2023/1543 displace Polish provisions of the Criminal Procedure Code (CPC) in the area of requesting electronic evidence from a provider residing in another Member State, which might have formed the basis for issuing decisions (so far in the form of issuing a European

[12] E. Rotondo, *Is the EU's Use of Regulations Becoming a Trend?*, 24.7.2013, http://publicsectorblog.practicallaw.com/is-the-eus-use-of-regulations-becoming-a-trend (access: 14.12.2024). See also R. Baldwin, M. Cave, M. Lodge, *Regulation and the European Union*, [in:] *Understanding Regulation: Theory, Strategy, and Practice*, eds. R. Baldwin, M. Cave, M. Lodge, Oxford 2011, pp. 388–408.

[13] Judgment of the CJEU of 7 November 1972 in case no. 20/72, *NV Cobelex v Rechtbank van Koophandel Antwerpen*, ECLI: ECLI:EU:C:1972:94; judgment of the ECtHR of 2 February 1977 in case no. 5/76, *Amsterdam Bulb BV v Produktschap voor Siergewassen*, ECLI: ECLI:EU:C:1977:13.

[14] Judgment of the CJEU of 1 March 1973 in case no. 40/69, *Paul G. Bollmann Company and Hauptzollamt Hamburg-Waltershof*, ECLI: ECLI:EU:C:1970:12. See also D. Kornobis-Romanowska, [in:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, ed. A. Wróbel, vol. 3, Warszawa 2012, p. 615.

[15] Judgment of the CJEU of 10 October 1973 in case 34/73, *Fratelli Variola S.p.A. and Amministrazione Italiana delle Finanze*, ECLI: ECLI:EU:C:1973:101.

Investigation Order).[16] Beginning from the date when Regulation 2023/1543 enters into force on 18 August 2026, its provisions will be directly applied by Polish courts and other procedural authorities. Moreover, as regulations may directly impose obligations on individual entities and Member States, also Polish service providers are obliged to enforce and execute obligations. This is done through the application of the provisions of the regulations by the competent authorities of the Member States, including courts.[17]

Therefore, when Regulation 2023/1543 states in Article 4 (1) (a) that a European Production Order to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user may be issued only by a judge, a court, an investigating judge or a public prosecutor competent in the case concerned, it gives a direct foundation for a decision issued by a Polish court which should indicate in the body of the decision that it has been issued on the basis of this Regulation. The competence of the Polish authorities must be derived straight from Regulation 2023/1543, not from the CPC – unless the Regulation explicitly states that some matters should be regulated in national law, and in some cases it does, as in the case of applicability of national system of remedies and national rules of admissibility of evidence. This model of direct application of regulation's provisions may cause problems since the structure of cooperation and notions used in Regulation 2023/1543 are not fully compatible with the system used in the Polish CP C. However, they are compatible with the law of the EU and allow for the uniform use and application all across the EU Member States – and that was the reason this solution was adopted. This aspect should create more homogeneity in the system, however a number of important aspects – in particular sanctions for service providers and remedies for individuals – are left to the Member States' legislations.

At the same time, the ban on transposition does not mean that no changes in the national law can be made. As a matter of fact, there is an obligation to adapt national provisions so that the direct application of a regulation is possible – in order to ensure the "operational framework". Two areas of legislation must be provided: first, provisions that allow for effective execution of powers enshrined in the regulation, and second, solutions that according to the regulation belong to the area of regulation of national law – in every case a given regulation states that some situation should be solved "in accordance with its national law", "according to the applicable national law". Such actions should be undertaken by every Member State in order

[16] This will be the second UE regulation that the Polish courts will have to apply directly, besides Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ EU L 303/1, 28.11.2018).

[17] See also M. Szwarc-Kuczer, *Zasada bezpośredniej skuteczności prawa wspólnotowego – wprowadzenie i wyrok ETS z 17.09.2002 r. w sprawie C-253/00 Antonio Munoz y Cia SA i Superior Fruiticola SA przeciwko Frumar Ltd i Redbridge Produce Marketing Ltd*, "Europejski Przegląd Sądowy" 2007, vol. 3, pp. 60–62.

to ensure effective application of the regulation, since "where the EU institutions have made a deliberate choice of a regulation as a method of harmonising laws, it means that any measures adopted by member states which put obstacles in the way of the effective achievement of the aims of those regulations may, depending on the circumstances in each case, risk falling foul of those regulations".[18]

PROBLEM OF EQUIVALENCE AND THE POLISH PROVISIONS IN FORCE

Regulation 2023/1543 is the next step in the development of common area of justice in the EU and offers a response for problems with specific character of criminality. The reason it had to be introduced was not lack of border controls for the criminals that can cross them freely but lack of borders in cyberspace – these can also be crossed without any control: "It is not the population that moves, but services are placed in other countries than their users".[19]

On the one hand, the e-evidence package is not restricted to "foreign" cases. In many cases an EPO will be used in purely domestic cases, so the scope of application may be far wider than it may seem now. On the other hand, it can be issued only to obtain foreign evidence – only orders directed to service providers residing in other Member States can be issued on the basis of the Regulation: "This Regulation should be applicable in all cross-border cases where the service provider has its designated establishment or legal representative in another Member State" (Recital 18 of the Preamble). The question arises whether the internal legal order should provide for the same powers of Polish procedural authorities in purely national cases, where the service provider resides in Poland. In such cases the Regulation will not applicable.

The question that arises here is whether there should be "new" national legislation that could provide for similar solutions. Actions taken on the basis of national law should not lead to discrimination in relation to actions taken on the basis of EU regulation – especially when it comes to remedies.[20] The powers of the judicial organs should be similar, allowing to obtain electronic evidence in the meaning of the Regulation on equal legal terms both from foreign and domestic service providers. The main difference would be that the purely national cases (double-national,

[18] See E. Rotondo, *op. cit*.

[19] 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), pp. 161–183; J.P. Mifsud Bonnici, M. Tudorica, J.A. Cannataci, *op. cit.*, p. 224.

[20] K. Lenaeerts, *National Remedies for Private Parties in the Light of the EU Law Principles of Equivalence and Effectiveness*, "Irish Jurist. New Series" 2011, vol. 46, p. 16.

as both the case is national and the provider is) the provisions of the Polish CPC would be applicable, not the Regulation.

Presently the Polish CPC regulates the stage of gathering electronic data (although it does not provide for legal rules of admissibility of evidence) – providing legal basis for two investigative measures. Firstly, the procedure of acquiring digital data by procedural authorities from individual private providers and service providers (regulated in Chapter 25 CPC as search and seizure) relates to the stage that can be an equivalent to a "production order". Secondly, the CPC introduces the obligation of service providers to secure certain digital data on the basis of a type of a "preservation order".

Article 236a CPC regulates the grounds for the production order. It enables search and seizure of IT systems. It stipulates that the provisions of this Chapter (Chapter 25: "Search and seizure") shall apply *mutatis mutandis* to the disposer and user of a medium containing IT data or an IT system, with respect to data stored in this device or system or on a medium at his disposal or use, including correspondence sent by e-mail. Thus, Article 236a CPC constitutes the legal basis for production and preservation of IT data stored: in an IT device; in the IT system; on a server; on an information medium, including correspondence sent by e-mail. The provision applies both to the disposer and the user of the IT system. The notion of "disposer of an IT system" in the Polish-language version can be understood also as a service provider in the meaning of the Regulation (although the notion of "disposer" used to describe the obliged entities is certainly not clear enough). The disposer, according to the literature, is a person authorized to manage the system, has the system at his disposal, and disposes of it at his discretion. The scope of the above-mentioned provisions extends to persons within whose reach the data in question are located. They do not have to be located in the place of residence of a specific person, as long as they can send, edit, copy, etc. This data may also be located outside Poland, e.g. on a foreign server.[21] The user is a person who uses the system, takes advantage of it, exploits it, derives some benefits from someone else's system, e.g. the holder of an e-mail account.[22] This concerns the network administrator and the computer user, who may possess information useful for the ongoing proceedings.

On the basis of this provision the following investigative measures will find application to electronic evidence.

1. Search of an IT system (Article 219 CPC).

2. Seizure of evidence (Article 217 CPC). The method of seizure on the basis of Article 217 in conjunction with Article 236a CPC relates only to data in the IT

[21] J. Skorupka, [in:] *Kodeks postępowania karnego. Komentarz*, ed. J. Skorupka, Warszawa 2023, p. 611.

[22] A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, "Prokuratura i Prawo" 2003, no. 10, p. 20; idem, *Dowody…*, p. 97.

system, not data from providers.[23] Files stored may, depending on the circumstances and technical possibilities, be seized together with the hardware or seized without the medium, or copied. In order to find them, first a search of the IT system, its parts, devices or media containing data may be carried out (Article 219 in conjunction with Article 236a CPC[24]). The person whose property is being searched cannot be required to print data, provide specialized devices or software, provide passwords – seizure is only possible in the scope of data available in the IT system that is undergoing the search.[25]

It is important to define the scope of data that can be seized on this basis. The Regulation 2023/1458 applies only to four types of stored. These can be grouped into two categories: the first group are "subscriber data" and "data requested for the sole purpose of identifying the user", which are considered less intrusive, and the second group are "traffic data" (except for data requested for the sole purpose of identifying the user) and "content data" (their detailed definitions may be found in Article 3 (9) to (12) of the Regulation). This signifies that outside the scope of the Regulation are live communications, interception of digital data in a network (e.g. Internet) and computer-assisted search.[26] But even this narrow scope gives the authorities the access to the content of communication and accumulated huge amounts of metadata to these communications.

At the same time the Polish provisions in Article 236a CPC are much wider: they relate to all data understood as a representation of facts or concepts communicated in a formalized way[27] and a medium is understood as any means of transporting data carrying any information.[28] Later, the data from the provider may be seized (only in a limited scope, however) on the basis of Article 218 in conjunction with Article 236a CP C. However, the fact that national regulations have a broader scope does not mean that national regulations remain inconsistent.

3. Seizure of data (Article 218, in the following scope resulting from the Act of 16 July 2004 – Telecommunications Law, Articles 180c and 180d: 1) determining the network termination point, telecommunications terminal device, end user: a) initiating the connection, b) to whom the connection is directed; 2) specifying:

---

[23] Idem, *Dowody…*, p. 110; idem, *Gromadzenie dowodów elektronicznych…*, p. 22.

[24] Idem, *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, "Prokuratura i Prawo" 2005, no. 10, p. 57.

[25] Idem, *Gromadzenie dowodów elektronicznych…*, p. 21.

[26] J.P. Mifsud Bonnici, M. Tudorica, J.A. Cannataci, *op. cit.*, p. 216.

[27] A. Lach, *Dowody…*, p. 20.

[28] P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, p. 46; W. Jasiński, *O potrzebie zmian w regulacjach prawnych dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, p. 56.

a) the date and time of the call and its duration, b) the type of call, c) the location of the telecommunications terminal device).

When it comes to activities exercised on the basis of Article 218 CPC in conjunction with Article 236a CPC, it is important to distinguish between the content and non-content data, when deciding about a particular legal ground for an investigative measure. Article 218 § 1 CPC can be applied when it comes to non-content data – such as establishing an IP address, the time and place of the connection. As a rule, a separate legal ground should be required with the so-called "content--data" – that is when the content of verbal messages, or recorded image and sound records, is transmitted. Then it is necessary to apply to the court to issue a decision on interception of communications in accordance with Article 237 §§ 1and 2 CPC.[29] Article 237 CPC is applied in conjunction with Article 241 CPC, which states that the provisions of this Chapter (this time Chapter 26: "Control and interception of communications") shall apply accordingly to the control and recording by technical means of the content of other conversations or information transmissions, including correspondence sent by e-mail.

Therefore, Article 237 in conjunction with Article 241 CPC constitutes the basis of intercepting "content" of electronic communications by the providers, that can be applied, according to A. Staszak and J. Kudła, to "cloud computing service – to the data located on the virtual disk allowing image and sound reproduction". In this case, it does not matter whether these conversations are conducted verbally (then the image and sound are recorded, the image itself is recorded, the sound itself is recorded) or in writing (via e-mail or programs used as part of e-mail intended also for to conduct conversations in speech and writing). This provision relates to a broad understanding of the concept of conversations, that A. Staszak and J. Kudła describe shortly as "substitutes for telephone calls". Basing on the necessity to distinguish between the content and non-content data and the use of different legal grounds of seizure, the authors propose rightly to apply a clear division between these two legal grounds for seizure of two types of data. In the case of non-content data (e.g. establishing an IP address, providing an e-mail address) it is sufficient to apply Article 218 § 1 CPC. However, a separate scope of the so-called "data" is an e-mail transmission service, when the content of messages (or an image or sound records) is transmitted. Then it is content data and it is necessary to apply to the court for control and recording of conversations in accordance with Article 237 §§ 1 and 2 CPC in conjunction with Article 241 CPC.[30]

This – it would appear – clear division between the two types of electronic data: content and non-content, is not clear in the Polish legal system and actually can be

[29] See J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, "Prokuratura i Prawo" 2017, no. 7–8, pp. 31–57.

[30] See also M. Kusak, *Dostęp…*, p. 46.

only derived from legal provisions in the process of systemic interpretation. The division between legal grounds for seizure of content data and non-content data is distorted as Article 236a CPC applies also to "correspondence sent by e-mail". It means that Articles 217–219 CPC can be applied also to search and seizure of such correspondence that is already in the IT system of a certain computer and its user – although without any doubt this could be understood as content data, as it relates to communications that are being stored in an IT system. This distortion is caused by the fact that a copy of a letter sent via e-mail can be saved in several places at the same time: on the sender's computer, on the sender's mail server, at the Internet service provider, on the recipient's mail server or on the recipient's computer,[31] but also in the area of cloud computing: key service operator and digital service provider and virtual disks, which would lead to securing specific data processed in the area of cloud computing.[32] Therefore, as the whole content of communications may be stored on an IT device or a medium, it means that law enforcement authorities can gain access to the content of communications (being substitutes of telephone conversations) in accordance with a standard analogous to the search in real world (Article 220 § 3 CPC), whereas the scale of invasion of privacy is similar to interception of communications (concerning content data).

W. Jasiński calls this structure adopted by the legislator "an analogy from the pre-digital world" and comes to the conclusion that this structure is not adequate to the method of communication in a digital environment. Also this author opposes to the use of this provision to content data, stressing that the acquisition of "static" data, i.e. data collected on specific media, should be regulated in a manner analogous to search activities, and in the case of "in motion" (live) communication, is should be managed according to the standard appropriate for the control and recording of conversations (Articles 236a and 241 CPC).[33]

In view of the Regulation entering into force, the most important task for the legislator seems to be establishing a clear division between content data and other types of electronic evidence. It should be clear that under Article 236a CPC it is not permitted to obtain the content of correspondence sent by e-mail. The standard of seizure of electronic conversations should not be lower compared to the control and recording of live phone conversations. It is clear that there is a need to change this chaotic legislative attitude and disregard towards the need to distinguish between these two types of data. Obtaining content data always requires a court's decision.

Article 218a CPC introduces a "preservation order". It provides that offices, institutions and entities conducting telecommunications activities or providing services by electronic means and digital service providers are obliged to immediately

[31] A. Lach, *Dowody elektroniczne w procesie…*, p. 33.

[32] See J. Kudła, A. Staszak, *op. cit.*, pp. 31–57.

[33] See W. Jasiński, *op. cit.*, p. 59; M. Kusak, *Dostęp…*, pp. 77–78.

secure, at the request of the court or the prosecutor for a specified period of time, not exceeding 90 days, IT data stored in devices containing this data on a carrier or in the IT system. The scope of the data provided to the state authorities is very narrow. It is stipulated in the Act of 16 July 2004 – Telecommunications Law, Articles 180c and 180d, and covers the same data as in the case of Article 218 in conjunction with Article 236a CPC. Also, securing data on request of the judicial authority is applied appropriately to secure content published or made available electronically. The entity obliged to comply with the request of the court or prosecutor may also be the content administrator (Article 218a § 3 CPC). As a result, this provision applies both to content data and non-content data. Article 236a CPC (that applies only to the stage of production of evidence) does not apply to this provision, Article 218a CPC can be applied directly.

This provision is directed to "offices, institutions and entities conducting telecommunications activities" not individuals. It also obliges these entities to "secure" data, not "transfer" or "reveal" them. The purpose of this provision is to secure data that may have evidentiary value and to maintain their integrity until further procedural steps are taken, usually issuing a decision to seize the data – on the basis of Article 217 CPC.[34] Thus, securing IT data is a kind of temporary measure preceding a possible request for their seizure (Article 217 § 1 in conjunction with Article 236a CPC). In order to carry out further activities, other legal grounds must be used.

On the basis of Article 218a CPC, IT data is secured only on the basis of a court decision or, in an investigation, a prosecutor. The Police and other bodies authorized to conduct an investigation, even if there is an emergency, do not have such authority. These authorities may request a prosecutor to issue such a decision (Article 326 § 3 CPC). The decision should clearly specify the scope of data that should be secured, e.g. by specifying the entities to which they concern, the subject of security, time and method of security, so that the data can be used in criminal proceedings.[35] At the same time seizure of these data – on the basis of Article 217 CPC – can be done also by the Police. This distinction does not have any rational explanation.

In 2021 the "preservation order" was supplemented by "preventing access procedures".[36] According to Article 218a § 1 second sentence CPC, in cases of crimes specified in Article 200b (promoting pedophilia), Article 202 §§ 3, 4, 4a and 4b (public display of pornographic content) or Article 255a (dissemination of content that may facilitate the commission of a terrorist crime) of the Criminal Code and in Chapter 7 of the Act of 29 July 2005 on counteracting drug addiction (production, processing,

[34] A. Lach, *Karnoprocesowe instrumenty…*, pp. 52–62.

[35] J. Skorupka, *op. cit.*, p. 590.

[36] Article 218a § 1 CPC amended by Article 3 (2) (a) of the Act of 20 April 2021amending the Act – Criminal Procedure Code and certain other acts (Journal of Laws 2021, item 1023) amending this Act as of 22 June 2021.

sale, transport, export, introduction to the market, supply of narcotic drugs and psychotropic substances) securing data may be combined with the obligation to prevent access to this data. In § 4 a "take down procedure" was established: if the publication or sharing of the content constituted a prohibited act (referred to in § 1), the court or prosecutor may order the removal of this content, imposing the obligation to comply with the provision on the service providers or administrators.

Taking into consideration the need to ensure equivalence with Regulation 2023/1458 model of freezing and obtaining electronic evidence it should be suggested that the provisions introducing production order and preservation order should be re-written. A clear structure of tools applicable in case of gathering and securing electronic evidence is needed. The present state of law in Poland reveals chaotic attitude, being a result of a hasty action of the legislator, attempting to follow the needs of prosecuting authorities. The interception of electronic evidence – also in the area that needs to be regulated in national law in order to comply with the obligations stemming from Regulation 2023/1458 (such as remedies) – relies on "applying accordingly" "regular provisions" applicable in "real-life", analogue world. This attitude is not sufficient and effective: "The Polish legislator permanently remained in the analogue world, not noticing what changes digitalization has brought to everyday (including criminal) life".[37] There is just one provision – Article 218a CPC – adequately related to electronic evidence, but this is just a partial solution.

A new structure for electronic evidence should be provided, equivalent with the model adopted in Regulation 2023/1458 and the production of electronic evidence from domestic service providers. The best solution would be to introduce a separate legal ground for investigative activity in the form of seizing electronic evidence – taking into consideration different environments where that can be executed; this provision would have to take into consideration the grounds to search for, freeze and seize evidence by service providers. It should also give adequate powers to seize data available in open sources.[38]

THE RIGHT TO AN EFFECTIVE REMEDY

Article 18 of Regulation 2023/1543 provides for "effective remedies". First, any person whose data were requested via an EPO shall have the right to effective remedies against that order. Secondly, where that person is a suspect or an accused

[37] W. Jasiński, *op. cit.*, p. 59. Otherwise, wrongly, see P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, "Prokuratura i Prawo" 2020, no. 9, p. 126.

[38] On the same topic, see P. Lewulis, *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, "Prokuratura i Prawo" 2022, no. 33, p. 144; W. Jasiński, *op. cit.*, p. 69; M. Kusak, *Dostęp…*, pp. 84–85.

person, such person shall have also the right to effective remedies during the criminal proceedings in which the data were being used. As the Regulation requires in Article 18, the remedy shall include the possibility of challenging the legality of the measure, including its necessity and proportionality, without prejudice to the guarantees of fundamental rights in the enforcing State. The Regulation furthermore requires that the same time limits or other conditions for seeking remedies in similar domestic cases shall apply for the purposes of this Regulation and in a way that guarantees that the persons concerned can exercise their right to those remedies effectively.

According to the attitude adopted in the Regulation, the national law should be the only source of remedies, not the EU law. It results, that the right to remedy can be only exercised before a court in the issuing State in accordance with its national law. It should be both available to any person, whose rights the order infringed and the suspect/accused, if in the proceedings concerning his/her criminal responsibility, electronic evidence obtained by the way of an EPO. The persons involved should be effectively and timely informed about the existing remedies.

The Polish law provides for the first type of remedies – "for any person whose data were requested via a European Production Order". Persons whose rights have been violated may lodge an interlocutory appeal against the decision regarding the search, seizure of property and physical evidence, as well as other activities; a complaint against a decision issued or an action taken during an investigation is heard by the district court in whose district the proceedings are conducted (Article 236 CPC). An interlocutory appeal is provided against the decision on search and seizure (the "production order" based on Articles 217 and 218 in conjunction with Article 236a CPC) and the decision on the basis of Article 218a CPC (the preservation order). However, there is no consent in the literature – some authors do not allow an appeal against a decision to secure IT data,[39] arguing that Article 236 CPC allows for an appeal against other actions relating to search, seizure of goods and physical evidence, but ignores securing them on the basis of Article 218a CPC (which is the basis not for production but preservation). Notwithstanding, this lacuna should be considered to be an omission of the legislator and it should be claimed that there is a possibility to appeal this decision under Article 236 CPC.[40] It is necessary in the view of the obligation stemming from Regulation 2023/1458 to provide a remedy to issuing an EPO. It can be derived from Article 236 CPC, however, it should be clearly stated, that also decision on issuing an EPO and EPrO, search and seizure of electronic evidence can be appealed.[41] Therefore, in this area another legislative change is needed.

[39] P. Hofmański (ed.), E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz*, Warszawa 2007, p. 1018; T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Warszawa 2014, p. 787.

[40] J. Skorupka, *op. cit.*, p. 590.

[41] J. Grajewski, S. Steinborn, L.K. Paprzycki, *Kodeks postępowania karnego. Komentarz*, Warszawa 2013, p. 727.

What about effective remedies for a person who is a suspect or an accused during the criminal proceedings? In an investigation, pursuant to Article 302 § 1 CPC, persons who are not parties may appeal against decisions and orders violating their rights; parties and non-parties may appeal only against actions other than decisions and orders violating their rights. The criterion for appealing against decisions, orders and other actions by persons who are not parties is only a direct violation of their rights. It leads to the conclusion that any person whose data were requested via an EPO can use this provision to appeal that order – both suspects and other persons. Article 302 § 1 CPC contains a supplementary clause constituting the basis for filing an interlocutory appeal when no other provision expressly provides for the appealability of the decision or order.[42] It can be used then only when Article 236 § 1 CPC does not provide for a ground of appeal. Additionally, § 2 allows for the possibility of filing an interlocutory appeal also against actions other than decisions and orders, and therefore also against the manner in which they were carried out.

When it comes to remedies available during the trial stage – provided for the person, who is a suspect or an accused person – there are none. In the trial stage only Article 236 § 1 CPC can be used – but only in a certain material scope. In the Polish procedure, there are no remedies available during trial for the parties against evidentiary actions, there is only an appeal against a judgment possible. There is no appeal against a decision of the court to introduce a piece of evidence (also EPO-based): its admissibility or legality, proportionality and necessity to use coercive methods; there is also no appeal against a decision not to introduce evidence. This is a serious lacuna in the Polish model procedure, limiting rights of the parties, especially defence, that has no right to effectively undermine the legality of evidence in criminal trial.

Moreover, one may question, how effective any remedy can be in the view of possibility to postpone the information about issuing an EPO? According to Regulation 2023/1458, the issuing authority should be able, in accordance with national law, to delay or restrict informing or omit to inform the person whose data are being requested, in which case the issuing authority should indicate in the case file the reasons for the delay, restriction or omission and add a short justification in the EPO certificate (Article 13 (2) of the Regulation).[43] The national law in the case of the Polish CPC is located in Article 218 § 2 CPC (used in conjunction with Article 236a CPC) which states that delivery of the decision may be postponed for

[42] *Ibidem*; S. Zabłocki, *Postępowanie odwoławcze w nowym kodeksie postępowania karnego*, Warszawa 1997, p. 171; A. Jaskuła, *Zaskarżalność postanowień w przedmiocie dowodów rzeczowych*, "Prokuratura i Prawo" 2009, no. 9, p. 38.

[43] Potential problems with this solution are discussed by A. Juszczak, E. Sason, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence*, "Eucrim" 2023, no. 3, p. 193.

a specified period of time necessary for the good of the case, but no later than until the final conclusion of the proceedings. It thus allows to delay informing the person interested in the case of seizure of data (similarly provides Article 239 in conjunction with Article 241 CPC in relation to interception of communications, also in digital environment). It does not allow, however, not to inform the person at all.[44]

Systemic change is needed in the area of remedies. They do not fulfill effectively the role in the light of requirements as set out by Regulation 2023/1458. It must be stressed that the remedy must be constructed in such a way that will be in accordance with Article 47 of the Charter of Fundamental Rights of the European Union.[45] The Charter applies in situations where Member States introduce measures aimed at implementing obligations imposed by a normative act defined by EU law. The Charter, and in particular its Article 47 also applies to ensure the full effectiveness of the actual rights that EU law confers on individuals.[46] The effectiveness of the remedy should be evaluated on the basis of its effectiveness in the meaning of Regulation 2023/1458.

THE SCOPE OF CONTROL OF THE COURT

The results of an EPO come back as information to the judicial organ of the issuing state and are presented in trial in the procedural form of evidence. With the model of operating of an EPO, the national court is the last and only resort to execute a total control of legality, necessity and proportionality, and the guarantees of fundamental rights – since Regulation 2023/1543 dispenses with the layer of judicial control and scrutiny while executing EPO request for evidence in the executing Member State. It delegates control over compliance with fundamental rights during execution of an EPO to the private sector – placing on them "undue responsibility".[47] This instrument is not based on the principle of equality and mutual trust – private providers do not enjoy equality with public authorities in terms of cooperation; this is evident by the very fact that they are subject to sanctions if they infringe their obligations under Regulation 2023/1458. Therefore, it may be perceived as bypassing the mutual legal assistance safeguards and the layers of fundamental rights scrutiny they entail.[48] In consequence, the only forum available for the interested person to request the control of both prerequisites of issuing an EPO and compliance with procedural rights, is the adjudicating court, as an EPO

[44] See judgment of the ECtHR of 28 May 2024 in case no. 72038/17 and 25237/18, *Pietrzak et Bychawska-Siniarska et Autres c. Pologne*.

[45] OJ C 364/1, 18.12.2000.

[46] K. Lenaerts, *Trybunał Sprawiedliwości Unii Europejskiej a ochrona praw podstawowych*, "Europejski Przegląd Sądowy" 2013, vol. 1, pp. 4–16.

[47] V. Mitsilegas, *op. cit.*, pp. 263–265.

[48] *Ibidem*.

may be issued only in certain circumstances and in certain scope of crimes and may apply only to a certain scope of data. The burden of control of compatibility with prerequisites of issuing an EPO, both *ex officio* and on request of parties, resulting from Regulation 2023/1458, is placed on this court.

The first prerequisite undergoing analysis would be the competence of a specific procedural authority to issue the EPO. The Regulation covers the data categories of subscriber data, traffic data and content data. As it was explained earlier, the categorization of data is directly linked to the conditions of issuance of EPOs and the circles of competent authorities. Obtaining content data is subject to stricter requirements to reflect the more sensitive nature of such data. A prosecutor may issue an EPO only to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user. An EPO to obtain traffic data, except for data requested for the sole purpose of identifying the user or to obtain content data may be issued only by a judge, a court or an investigating judge. In such a case, the EPO issued by a prosecutor should be validated, after examination of its conformity with the conditions for issuing an EPO under this Regulation, by a judge, a court or an investigating judge in the issuing State. A content-data EPO issued by a prosecutor without validation of a judge, mistakenly executed by the requested service provider, should be considered invalid. Obtained evidence in such a case is illegal – in the meaning of lacking legal basis for action of state authorities.

The control of the court may be particularly important in the cases where it is not clear whether the EPO for an IP address relates to content data or non-content data. It can be both data requested for the sole purpose of identifying the user or to obtain content data. Under certain circumstances, IP addresses can be considered traffic data. However, where IP addresses, access numbers and related information are not requested for the sole purpose of identifying the user in a specific criminal investigation, they are generally requested to obtain more privacy-intrusive information, such as the contacts and whereabouts of the user. As such, they could serve to establish a comprehensive profile of an individual concerned, but at the same time they can be processed and analysed more easily than content data, as they are presented in a structured and standardised format. It is therefore essential that, in such situations, IP addresses, access numbers and related information not requested for the sole purpose of identifying the user in a specific criminal investigation, be treated as traffic data and requested under the same regime as content data, as defined in Regulation (Recital 33 of the Preamble).

Assessing the premises that make it legal to issue an EPO, the court should also check other prerequisites resulting from the Regulation, that are decisive in the process of analysing admissibility of electronic evidence.

1. If EPO was issued in the proper scope of criminal offences.

An EPO to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user may be issued for all criminal offences and for the execu-

tion of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered *in absentia*, in cases where the person convicted absconded from justice. An EPO to obtain traffic data, except for data requested for the sole purpose of identifying the user or to obtain content data should only be issued for certain criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years, if they are wholly or partly committed by means of an information system. This restriction eliminates some offences from the scope of application of the orders for traffic and content data.[49]

2. If the execution of the EPO could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State.

The EPO should not interfere with both national law on immunities and privileges and the law of the state where the service provider resides. Issuing authority should oblige the immunities and privileges, according to the applicable national law, which may refer to categories of persons, such as diplomats, or specifically protected relationships, such as lawyer-client privilege or the right of journalists not to disclose their sources of information. Moreover, the issuing authority should only be able to issue the order if it could have been issued under the same conditions in a similar domestic case. Limitations to investigative activities against certain groups of persons are contained in national exclusionary rules. In a case, where the EPO could infringe the immunities and privileges in the law of the provider, the addressee should inform the issuing authority and the enforcing authority.

This requirement is especially important for the protection of individuals. Large part of criticism directed against Regulation 2023/1458 related to the risk that this law enforcement instrument may be abused to target journalists, human rights defenders, activists, political opponents and lawyers.[50] The adjudicating court should thus prevent a danger that this instrument of extracting data about users and their communications may be used as a part of systemic abuse of state surveillance powers.

3. If the EPO issued was necessary, proportionate, adequate and applicable to the case at hand.

The issuing authority should take into account the rights of the suspect or the accused person in proceedings relating to a criminal offence and should only issue an EPO if such order could have been issued under the same conditions in a sim-

[49] See S. Tosza, *The E-evidence Package…*, p. 167.

[50] See C. Berthélémy, *E-evidence Compromise Blows a Hole in Fundamental*, 2023, https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards (access: 14.12.2024).

ilar domestic case. The assessment of the adjudicating court should also take into account whether such EPO is limited to what was strictly necessary to achieve the legitimate aim of obtaining data that are relevant and necessary as evidence in an individual case.

4. If the right of defence and fairness of the proceedings was respected.

In Article 18 (5) the Regulation provides that without prejudice to national procedural rules, the issuing State and any other Member State to which electronic evidence has been transmitted under this Regulation shall ensure that the rights of defence and fairness of the proceedings are respected when assessing evidence obtained through the EPO. Here it should be pointed out that in the Polish CPC, the defence has no real and effective opportunity either to get an EPO issued (they can only lodge a non-binding request to the court or a prosecutor). Moreover, there is no procedure in which the defence could request that the evidence contained in the case-file be declared inadmissible. The defence can make a free (not regulated in the CPC) motion during trial to exclude illegally obtained evidence (also EPO-based) – however, there is no obligation on the part of the court to react to this motion. For the defence the best strategy would be to remember that all data categories contain personal data and are covered by the safeguards under the Union data protection acquis, e.g. it is possible to seek remedies under Regulation (EU) 2016/679[51] and Directive (EU) 2016/680.[52]

5. If fundamental rights and legal principles as enshrined in the Charter and in Article 6 TEU were guaranteed in the procedure.

Article 1 (3) of Regulation 2023/1458 stipulates that this Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in the Charter and in Article 6 TEU, and any obligations applicable to law enforcement authorities or judicial authorities in this respect shall remain unaffected. The provisions of the Regulation should be applied without prejudice to fundamental principles, in particular the freedom of expression and information, including the freedom and pluralism of the media, respect for private and family life, the protection of personal data, as well as the right to effective judicial protection. This obligation leads to the question, what about orders issued by Member States with systemic rule of law deficiencies. The weak protections against fundamental rights violations will notably impact people

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119/1, 4.5.2016).

[52] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ EU L 119/89, 4.5.2016).

residing in Member States with systemic rule of law problems.[53] In such states EPO may be used as a "quasi-Pegasus", and serve as a tool to access data about, e.g., members of the opposition.

To sum up, the scope of analysis for the adjudicating court seems to be quite wide. Especially it will have to analyse these issues on request of the defence. With the direct route from the provider to the issuing Member States' courtroom – the only guarantor of compliance with rights is the court which adjudicates the case where the e-evidence is used. When the grounds for refusal are assessed by a non-judicial organ – the provider – it makes the task of the adjudicating court in its role as the supervisor of the defendant's rights, even more prominent. The question for the legislator or for the courts' case law is to decide whether such control should be executed *ex officio* or only on the request of the party.

ADMISSIBILITY OF EVIDENCE

Once electronic evidence are produced on the basis of EPO (earlier possibly preserved as a result of an EPrO) they may be presented as evidence in criminal trial in the state of the issuing authority. Regulation 2023/1458 does not refer to the admissibility of electronic evidence acquired on its basis. The only provision that refers to this topic is Article 20, which states that documents transmitted as part of electronic communication shall not be denied legal effect or be considered inadmissible in the context of cross-border judicial procedures under this Regulation solely on the ground that they are in electronic form. The Regulation refers the problem of assessing the admissibility of electronic evidence to national courts – but only in Preamble (Recital 17), not in the text of legal provisions, stating that in order to guarantee full respect of fundamental rights, the probative value of evidence gathered in application of this Regulation should be assessed in trial by the competent judicial authority, in accordance with national law and in compliance with, in particular, the right to a fair trial and the right of defence.

In consequence, rules concerning admissibility of evidence stems from both *lex fori* and *lex loci* principle. First, an EPO can be issued only in accordance with national law. Second, the provisions of Regulation 2023/1543 are based on the principle of mutual recognition, but only if the evidence was lawfully obtained in accordance with the *lex loci*. Therefore, this requirement can be perceived as one of the admissibility prerequisites. Care in respecting compliance with the *lex loci* thus becomes a requirement for the admissibility of evidence, that ensures the legality

[53] *Ibidem*. See also the scenarios and dangers elaborated in European Digital Rights, *Demonstrating Gaps in the e-Evidence Regulation*, 2021, https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_10_20_EDRI_eEvidence%20Scenarios.pdf (access: 14.12.2024), p. 193.

of its collection. It ensures that different legal frameworks are not an obstacle to the admissibility (use) of evidence obtained abroad. It provides also for some flexibility, allowing the forum State to activate a kind of emergency break and refuse the cross-border evidence if, despite complying with the *lex loci*, a fundamental principle of its constitution is violated. However, it does not refer to a situation where there are different standards in Members States as to the content data guarantees.[54]

There is a proposition to cover the lacuna in rules on admissibility of evidence in the EU prepared by the European Law Institute in a "Legislative Proposal on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings in the EU". The proposal, in accordance with information provided by the authors, "seeks to achieve this balance by establishing a general rule of admissibility of cross-border evidence, as long as the *lex loci* is complied with and no inalienable constitutional rights in the forum State are violated".[55] The proposal rightly observes that most legal systems of Member States do not regulate admissibility of transnational and foreign evidence in criminal proceedings on consistent and comprehensive rules. In some cases, it is admitted without any further question, whilst, in other cases, it is subject to exhaustive domestic filters aimed at ensuring compliance with domestic legal principles and sometimes also with the statutory provisions of the executing State. The divergence of rules, principles and practices certainly leads to increasing complexity of transnational justice. Specifically, the proposal deals with admissibility of electronic evidence.[56]

The first stage of dealing with electronic evidence is forming them into evidence in a procedural sense. "Electronic evidence" that Regulation 2023/1543 refers to in Article 1 is not evidence in a procedural meaning. Terminology chosen by the Commission – "electronic evidence" – could automatically imply that the data gathered is admissible as evidence in a criminal proceeding.[57] During the negotiations over the Regulation it was suggested to replace the term with "a more neutral terminology",

[54] M. Kusak, *Dostęp…*, p. 83.

[55] European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute*, approved by the ELI Council on 23 February 2023 and by the ELI Membership on 4 May 2023, final version published on 8 May 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf (access: 14.12.2024), p. 8.

[56] See also L. Bachmaier, *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?*, "Eucrim" 2023, no. 3, pp. 226–227.

[57] As observed by T. Christakis, *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Matters*, eds. V. Franssen, S. Tosza, Cambridge 2023, p. 9.

namely "electronic information".[58] However, this proposition was not taken into consideration. It is the task of the investigating authority, that should take care that these data and information would be shaped and formed as evidence and as such presented in a trial. Here, it is necessary to decide on what legal basis their admissibility should be evaluated.[59] Secondly, there is a need to evaluate their evidentiary value. The Polish Supreme Court stated that computer forensics is a dynamically developing field, which obliges judicial authorities to strive to obtain knowledge about the most perfect methods of securing evidence in a case.[60] However, securing electronic evidence by service providers leads to obtaining credible evidence and no special methods of verification must be used. It is the most credible and certain method of obtaining data electronically stored or exchanged, that results in clear and simple information (which does not mean that it cannot be undermined).

CONCLUSIONS

In the present state of law, Polish criminal procedure lacks proper structure of gathering of electronic evidence. The state authorities have to move among a haze of legal provisions, not sure what legal ground should be applied and not certain in what scope the "analogue" procedural measures can be applied in the digital environment. Moreover, when there is no clear structure of search and seizure (leading to production of) of electronic evidence, also the guarantees for individuals are not clear. As it was suggested before, taking into consideration the need to equivalently regulate gathering of electronic evidence, provisions introducing production order and preservation order should be re-written, in order to provide for clear structure of tools applicable in case of gathering and securing electronic evidence. There is a need to adopt a coherent standard for production of non-content and content data.

The present state of law reveals chaotic attitude, being a result of a hasty action of the legislator, attempting to follow the needs of prosecuting authorities. The interception of electronic evidence – also in the area that needs to be regulated in national law in result of entering into force Regulation 2023/1458 – relies on "applying accordingly" "regular provisions" applicable in the "real-life", analogue

[58] Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), rapporteur: Birgit Sippel, 24.10.2019, https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf (access: 14.12.2024), para. 147.

[59] On verification of electronic evidence, see D. Szumiło-Kulczycka, *Weryfikacja legalności i wiarygodności dowodów elektronicznych w kontradyktoryjnym procesie karnym*, "Gdańskie Studia Prawnicze" 2024, no. 2, pp. 90–95.

[60] Decision of the Supreme Court of 20 June 2013, III KK 12/13, LEX no. 1341691.

world. Thus, the Regulation, in order to be operational, requires better national legislation. A new structure for gathering electronic evidence should be provided, suitable both for the needs of Regulation 2023/1458 and the production of electronic evidence from domestic service providers. The best solution would be to introduce a separate legal ground for investigative activity in the form of seizing electronic evidence from the service provider – taking into consideration different environments where that can be executed. This provision would have to take into consideration the grounds to seize evidence by service providers.[61]

Second, there is a need of clear division between legal grounds for seizure of content data and non-content data in compliance with the clear structure established in the Regulation. Presently, is not clear in the Polish legal system and this division can be only derived from legal provisions in the process of systemic interpretation. In result, as the whole content of communications may be stored on an IT device or a medium, it means that law enforcement authorities can gain access to the content of communications in accordance with a standard analogous to the search in real world, whereas the scale of invasion of privacy is similar to interception of communications (when the search results in acquiring content data). It needs to be stressed that there should not be two standards applicable – the standard applicable to a national service provider being much lower than the one applied when data are EPO-based.

Third, there are serious lacunas in the Polish model procedure, limiting rights of the parties, especially defence, that has no right to effectively undermine the legality of evidence in criminal trial. There is no appeal against a decision of the court to introduce a piece of evidence (also EPO-based): its admissibility or legality, proportionality and necessity to use coercive methods. There is also no appeal against a decision not to introduce evidence. Such a tool should be provided for both parties, as formulating objections against legality of a piece of electronic evidence within an appeal against a judgment of a court cannot be considered to be an effective remedy in the meaning of Regulation 2023/1458.

Finally, the problem of admissibility of electronic evidence reflects all the most pressing problems of the Polish criminal procedure. It even makes them greater, revealing the chaotic attitude towards evidentiary rules. Also, there is a lacuna in the EU law in the area of admissibility of evidence gathered in another Member State. There is no specific regulation relating to this issue – as well as admissibility of electronic evidence. Therefore, every Member State decides how to assess the admissibility of such evidence and what rules of evidence apply in a specific procedural situation. This leads in turn to several problems with the standards of

[61] W. Jasiński (*op. cit.*, p. 61) rightly states that "in relation to the acquisition of digital data, the already poor guarantee of search provisions is additionally weakened by a rather general reference, which allows to further blur the meaning of regulations limiting interference with individual rights and freedoms".

admissibility of electronic evidence.[62] Presently, Polish courts are left with the obligation – and freedom – of assessment limited only by rules based on Article 7 CPC (taking into account the principles of correct reasoning and the recommendations of knowledge and life experience). The only direction as to the rules of admissibility is Article 6 of the European Convention on Human Rights and the notion of fair trial and they should be applied also in EPO cases.

There is no doubt that measures to obtain and preserve electronic evidence are increasingly important for criminal investigations and prosecutions across the Union. Regulation 2023/1458 offers a breakthrough tool of cooperation. However, there are no equivalent rules of gathering electronic evidence in the Polish national legal order. Firstly then, there is a need that the new rights and obligations stemming from the Regulation be analyzed by both domestic legislator and all the involved actors.[63] Secondly, it should give the national legislator the incentive to re-write the system of gathering and assessing applicability of electronic evidence for the purposes of national cases. It is the highest time to deal with this issue in a coherent way, harmonized with the EU law.

REFERENCES

Literature

Bachmaier L., *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?*, "Eucrim" 2023, no. 3, **DOI: https://doi.org/10.30709/eucrim-2023-019**.

Baldwin R., Cave M., Lodge M., *Regulation and the European Union*, [in:] *Understanding Regulation: Theory, Strategy, and Practice*, eds. R. Baldwin, M. Cave, M. Lodge, Oxford 2011.

Christakis T., *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Matters*, eds. V. Franssen, S. Tosza, Cambridge 2023.

Forlani G., *The E-evidence Package: The Happy Ending of a Long Negotiation Saga*, "Eucrim" 2023, no. 3, **DOI: https://doi.org/10.30709/eucrim-2023-013**.

Grajewski J., Steinborn S., Paprzycki L.K., *Kodeks postępowania karnego. Komentarz*, Warszawa 2013.

Grzegorczyk T., *Kodeks postępowania karnego. Komentarz*, Warszawa 2014.

Hofmański P. (ed.), Sadzik E., Zgryzek K., *Kodeks postępowania karnego. Komentarz*, Warszawa 2007.

[62] For example, see Request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 – Criminal proceedings against M.N., in case C-670/22, 2023/C 35/37; judgment of the CJEU of 30 April 2024 in case C-670/22, ECLI:EU:C:2024:372; J.J. Oerlemans, D.A.G. van Toor, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, "European Journal of Crime, Criminal Law and Criminal Justice" 2022, vol. 30, p. 315.

[63] See also A. Juszczak, E. Sason, *op. cit.*, pp. 192–193.

Jasiński W., *O potrzebie zmian w regulacjach prawnych dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.04**.

Jaskuła A., *Zaskarżalność postanowień w przedmiocie dowodów rzeczowych*, "Prokuratura i Prawo" 2009, no. 9.

Juszczak A., Sason E., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence*, "Eucrim" 2023, no. 3, **DOI: https://doi.org/10.30709/eucrim-2023-014**.

Kornobis-Romanowska D., [in:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, ed. A. Wróbel, vol. 3, Warszawa 2012.

Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, "Prokuratura i Prawo" 2017, no. 7–8.

Kusak M., *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.05**.

Kusak M., *Mutual Trust to Obtain Evidence in the EU: Is the Bar Law or High?*, [in:] *Current Issues of EU Criminal Law*, eds. A. Ochnio, H. Kuczyńska, Warszawa 2022.

Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.

Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, "Prokuratura i Prawo" 2003, no. 10.

Lach A., *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, "Prokuratura i Prawo" 2005, no. 10.

Lenaeerts K., *National Remedies for Private Parties in the Light of the EU Law Principles of Equivalence and Effectiveness*, "Irish Jurist. New Series" 2011, vol. 46.

Lenaerts K., *Trybunał Sprawiedliwości Unii Europejskiej a ochrona praw podstawowych*, "Europejski Przegląd Sądowy" 2013, vol. 1.

Lewulis P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, vol. 33, **DOI: https://doi.org/10.1007/s10609-021-09430-4**.

Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, **DOI: https://doi.org/10.31338/uw.9788323548027**.

Lewulis P., *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, "Prokuratura i Prawo" 2022, no. 3.

Mifsud Bonnici J.P., Tudorica M., Cannataci J.A., *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, [in:] *Handling and Exchanging Electronic Evidence Across Europe*, eds. M.A. Biasiotti, J.P. Mifsud Bonnici, F. Turchi, Cham 2018, **DOI: https://doi.org/10.1007/978-3-319-74872-6_11**.

Mitsilegas V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), **DOI: https://doi.org/10.1177/1023263X18792240**.

Oerlemans J.J., Toor D.A.G. van, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, "European Journal of Crime, Criminal Law and Criminal Justice" 2022, vol. 30, **DOI: https://doi.org/10.1163/15718174-bja10037**.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, "Prokuratura i Prawo" 2020, no. 9.

Pfeffer K., *Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln*, "Eucrim" 2023, no. 3, **DOI: https://doi.org/10.30709/eucrim-2023-012**.

Skorupka J., [in:] *Kodeks postępowania karnego. Komentarz*, ed. J. Skorupka, Warszawa 2023.

Szumiło-Kulczycka D., *Weryfikacja legalności i wiarygodności dowodów elektronicznych w kontradyktoryjnym procesie karnym*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.06**.

Szwarc-Kuczer M., *Zasada bezpośredniej skuteczności prawa wspólnotowego – wprowadzenie i wyrok ETS z 17.09.2002 r. w sprawie C-253/00 Antonio Munoz y Cia SA i Superior Fruiticola SA przeciwko Frumar Ltd i Redbridge Produce Marketing Ltd*, "Europejski Przegląd Sądowy" 2007, vol. 3.

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**.

Tosza S., *The E-evidence Package Is Adopted: End of a Saga or Beginning of a New One?*, "European Data Protection Law Review" 2023, vol. 9(2), **DOI: https://doi.org/10.21552/edpl/2023/2/11**.

Tosza S., *The European Commission's Proposal on Cross-Border Access to E-Evidence*, "Eucrim" 2018, no. 4, **DOI: https://doi.org/10.30709/eucrim-2018-021**.

Tosza S., *W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.03**.

Zabłocki S., *Postępowanie odwoławcze w nowym kodeksie postępowania karnego*, Warszawa 1997.

Online sources

Berthélémy C., *E-evidence Compromise Blows a Hole in Fundamental*, 2023, https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards (access: 14.12.2024).

Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), rapporteur: Birgit Sippel, 24.10.2019, https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf (access: 14.12.2024).

European Commission, *E-evidence – Cross-Border Access to Electronic Evidence*, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (access: 14.12.2024).

European Digital Rights, *Demonstrating Gaps in the e-Evidence Regulation*, 2021, https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_10_20_EDRI_eEvidence%20Scenarios.pdf (access: 14.12.2024).

European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute*, approved by the ELI Council on 23 February 2023 and by the ELI Membership on 4 May 2023, final version published on 8 May 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf (access: 14.12.2024).

Rotondo E., *Is the EU's Use of Regulations Becoming a Trend?*, 24.7.2013, http://publicsectorblog.practicallaw.com/is-the-eus-use-of-regulations-becoming-a-trend (access: 14.12.2024).

Legal acts

Charter of Fundamental Rights of the European Union (OJ C 364/1, 18.12.2000).

Consolidated version of the Treaty on the European Union and the Treaty on the Functioning of the European Union (OJ C 326/47, 26.10.2012).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities

for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ EU L 119/89, 4.5.2016).

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).

Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM(2018) 225 final.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119/1, 4.5.2016).

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ EU L 303/1, 28.11.2018).

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).

Case law

Decision of the Supreme Court of 20 June 2013, III KK 12/13, LEX no. 1341691.

Judgment of the CJEU of 7 November 1972 in case no. 20/72, *NV Cobelex v Rechtbank van Koophandel Antwerpen*, ECLI: ECLI:EU:C:1972:94.

Judgment of the CJEU of 1 March 1973 in case no. 40/69, *Paul G. Bollmann Company and Hauptzollamt Hamburg-Waltershof*, ECLI: ECLI:EU:C:1970:12.

Judgment of the CJEU of 10 October 1973 in case 34/73, *Fratelli Variola S.p.A. and Amministrazione Italiana delle Finanze*, ECLI: ECLI:EU:C:1973:101.

Judgment of the CJEU of 30 April 2024 in case C-670/22, ECLI:EU:C:2024:372.

Judgment of the ECtHR of 2 February 1977 in case no. 5/76, *Amsterdam Bulb BV v Produktschap voor Siergewassen*, ECLI: ECLI:EU:C:1977:13.

Judgment of the ECtHR of 28 May 2024 in case no. 72038/17 and 25237/18, *Pietrzak et Bychawska-Siniarska et Autres c. Pologne*.

Request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 – Criminal proceedings against M.N., in case C-670/22, 2023/C 35/37.

ABSTRAKT

W artykule skupiono się na problemach wynikających z przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności. Po wejściu w życie tego rozporządzenia (18 sierpnia 2026 r.) sądy krajowe będą mogły wykorzystywać w postępowaniu karnym dane uzyskane w wyniku europejskiego nakazu wydania dowodów elektronicznych oraz (na wcześniejszym etapie) europejskiego nakazu zabezpieczenia dowodów elektronicznych, a następnie oceniać ich dopuszczalność. Pakiet e-dowodów oferuje organom procesowym

narzędzie umożliwiające gromadzenie dowodów w formie elektronicznej. Jednocześnie w pakiecie tym nie wspomina się o tym, w jaki sposób te dowody – tak łatwo i szybko uzyskane od usługodawców w innych państwach członkowskich – powinny być traktowane przez sądy krajowe. Tymczasem jest to kluczowy etap oceny wyników tej współpracy dla organów wymiaru sprawiedliwości oraz może rodzić liczne problemy, zarówno prawne, jak i praktyczne. Dlatego w artykule przeanalizowano, jak wygląda pakiet e-dowodów z polskiej perspektywy oraz w jaki sposób polskie sądy mogą dopuszczać w procesie karnym dowody elektroniczne uzyskane od usługodawców na podstawie przepisów tego rozporządzenia. Ponadto zwrócono uwagę na problem bezpośredniego stosowania przepisów rozporządzenia oraz problem równoważności uprawnień organów krajowych wobec usługodawców mających siedzibę w innych państwach i wobec usługodawców mających siedzibę w Polsce. W tym obszarze przedstawiono analizę krajowych ram prawnych, której celem jest pokazanie, czy obecnie istnieją w polskim procesie karnym odpowiednie i równoważne podstawy prawne do wydawania nakazów wydania i zabezpieczenia dowodów elektronicznych w prawie krajowym wobec usługodawców krajowych. W wyniku przeprowadzonej analizy wykazano, że w celu zabezpieczenia i zapewnienia skutecznego stosowania rozporządzenia konieczne jest dokonanie zmian w polskim prawie karnym procesowym.

Słowa kluczowe: proces karny; dowody elektroniczne; europejski nakaz wydania dowodów elektronicznych; dopuszczalność dowodów; współpraca Unii Europejskiej w sprawach karnych