The EU “E-Evidence package” from the Polish perspective: the highest time for a systemic change (iThenticate Smilarity Report)

WORD COUNT	11793	TIME SUBMITTED	23-AUG-2024 08:26PM
		PAPER ID	111259910

Faculty of Law and Administration

STUDIA IURIDICA LUBLINENSIA

The EU "E-Evidence package" from the Polish perspective: the highest time for a systemic change

„Pakiet E-dowodów" w prawie Unii Europejskiej z perspektywy polskiej: najwyższy czas na systemową zmianę

ABSTRACT

The text focuses on problems resulting from adoption of the 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 finally. Once the Regulation enters into force (18 August 2026) national courts will be able to include data obtained as a result of issuing of an EPO (or earlier an EPrO) in the case file and then assess their admissibility. The "E-Evidence package" offers to the procedural authorities the 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 – are treated by national courts. And this is the stage that is decisive for justice systems and may lead to numerous – both legal and practical – problems. Therefore, the paper will deal 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, the text will also deal with a problem of direct application of regulation and the problem of equivalence of powers of national authorities towards service providers residing in other states and providers residing in Poland. In this area an analysis of national legal framework will be presented, that will show if there are presently adequate and equivalent legal grounds for issuing production and preservation orders in national law – towards national provid In the result of the conducted analysis it will be shown that several changes in the Polish law are necessary in order to secure and ensure the effective application of the Regulation.

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

ABSTRAKT

W tekście 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 Rozporządzenia (18 sierpnia 2026 r.) sądy krajowe będą mogły wykorzystywać z postępowaniu karnym dane uzyskane w wyniku wydania „europejskiego nakazu wydania dowodów elektronicznych" oraz (na wcześniejszym etapie) „europejskiego nakazu zabezpieczenia dowodów elektronicznych". „Pakiet E-dowodów" oferuje organom procesowym narzędzie umożliwiające gromadzenie dowodów w formie elektronicznej. Jednocześnie w pakiecie tym nie wspomina się o sposobie, w jaki te dowody – tak łatwo i szybko uzyskane od usługodawców w innych państwach członkowskich –powinny być traktowane przez sądy krajowe. A ten etap jest kluczowym etapem oceny wyników tej współpracy dla organów wymiaru sprawiedliwości, i może rodzić liczne problemy – zarówno prawne, jak i praktyczne. Dlatego też w artykule poruszony zostanie problem tego, jak wygląda „Pakiet E-dowodów" z polskiej perspektywy oraz w jaki sposób polskie sądy mogą dopuszczać w procesie karnym uzyskane od usługodawców na podstawie przepisów tego rozporządzenia dowody elektroniczne. Ponadto w tekście poruszony zostanie także 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 zostanie przedstawiona analiza krajowych ram prawnych, która pokaże, 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 wykazane zostanie, że w celu zabezpieczenia i zapewnienia skutecznego stosowania Rozporządzenia koniecznych jest dokonanie zmian w polskim prawie karnym procesowym.

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

I. Introduction

On 12 July 2023, after 5 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 was finally adopted[2]. 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 emails, 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 a European Production Order). The Regulation shall apply from 18 August 2026, which gives Members States and service providers 3 years to prepare the operational framework in order to comply with the new

CORRESPONDENCE ADDRESS: xxx

[1] See on the history of negotiations: 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. 2, p. 163. Also: G. Forlani, *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, „Eucrim" 2023/3, p. 174-181.

[2] Regulation (EU) 2023/1543 of the European Parliament and of the Council of the EU on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, pp. 118–180.

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 will focus on the problems that arise when national courts need to include data obtained as a result of issuing of an EPO (or earlier an EPrO) in the case file and then assess their admissibility[4]. The E-Evidence package offers to 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. And this is the stage that is decisive for justice systems and may lead to numerous – both legal and practical – problems. Therefore, the paper will deal 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, the text will also deal with a problem of direct application of regulation and the problem of equivalence of powers of national authorities towards service providers residing in other states and providers residing in Poland. In this area a thorough analysis of national legal framework will be necessary, that will show if there are presently legal grounds for issuing production and preservation orders in national law – towards national providers. In the result of the conducted analysis it will be shown 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 the Regulation 2023/1543 bases on a model of direct cooperation while excluding the need to contact judicial organs in the MS of

[3] 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 L 191, 28.7.2023, p. 181–190.
[4] See e.g. on the example of Germany: K. Pfeffer, *Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln*, „Eucrim" 2023/3, p. 170-171.
5 See: "E-evidence - cross-border access to electronic evidence Improving cross-border access to electronic evidence", at: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

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 MS: it is a "privatization of the mutual cooperation model"[6]. In consequence it is rather a tool to avoid cooperation with other MSs's 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 assessed by a non-judicial organ – the service provider. There is only a notification procedure possible (to executing MSs' 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 the Regulation. The Regulation presents a definition of "electronic evidence"; therefore, it is possible to distinguish "electronic evidence" from "digital evidence". According to Article 3(8) "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: 1/ stored in an electronic form either by the service provider or on its behalf; 2/ 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

[6] V. Mitsilegas, *Editorial. 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, COM (2018) 225 final.
[7] More on this topic in: S. Tosza, *The E-Evidence Package is Adopted*, p. 168.

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

It is also important to underline that "European Production Orders and European Preservation Orders 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. EPOs cannot be used as a tool of discovery of crimes, mechanism of looking for probable crimes, but only as a tool of acquiring evidence of already investigated crimes. Preamble explains this prerequisite even further, stating in motive 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".

---

[8] S. Tosza, *The European Commission's Proposal on Cross-Border Access to E-Evidence*, "Eucrim" 2018, vol. 4, at: https://eucrim.eu/articles/european-commissions-proposal-cross-border-access-e-evidence/.

[9] So far the two notions were understood identically, and the two words were used alternately. According to P. Lewulis, 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. P. Lewulis, *Collecting Digital Evidence From Online Sources: Deficiencies In Current Polish Criminal Law*, "Criminal Law Forum" 2022, vol. 33, p. 43. According to A. Lach, 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. See: A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 28-30.

II. Problems with direct application of a 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 Functioning of the European Union (TEU, C 326/47) 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[10]. 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 MS, provisions of regulations are applicable directly and take precedent over national 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[11]. 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[12]. 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

[10] J. P. Mifsud Bonnici, M. Tudorica, J. A. Cannataci, *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, in: M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, & F. Turchi (eds.), *Handling and Exchanging Electronic Evidence Across Europe*, Springer 2018, p. 193.
[11] E. Rotondo, Is the EU's use of regulations becoming a trend? Thomson Reuters Blog. 24/07/2013 at: http://publicsectorblog.practicallaw.com/is-the-eus-use-of-regulations-becoming-a-trend/; see also: R. Baldwin, M. Cave, M. Lodge, *Regulation and the European Union*, in: *Understanding Regulation: Theory, Strategy, and Practice*, R. Baldwin, M. Cave, M. Lodge (eds.), Oxford University Press 2011, pp. 388-408.
[12] Judgment of the Court of 7 November 1972, case no. 20/72, NV Cobelex v Rechtbank van Koophandel Antwerpen, ECLI: ECLI:EU:C:1972:94; Judgment of the Court of 2 February 1977, case no. 5/76, Amsterdam Bulb BV v Produktschap voor Siergewassen, ECLI: ECLI:EU:C:1977:13.

regulation[13]. 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, in case 34/73, *Fratelli Variola S.p.A. and Amministrazione Italiana delle Finanze*, the CJEU stated that the establishment of a national act that repeats the provisions contained in the regulation is *per se* a violation of EU law[14]. 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 the Regulation 2023/1543 displace Polish provisions of the Code of Criminal Procedure (CCP) 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 Investigation Order)[15]. Beginning from the date when the 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 execute obligations. This is done through the application of the provisions of the regulations by the competent authorities of the Member States, including courts[16]. Therefore, when the 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

[13] Judgment of the Court of 1 March 1973, 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. Tom III*, A. Wróbel (ed.), Warszawa 2012, p. 615.
[14] ECLI: ECLI:EU:C:1973:101.
[15] 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 L 303, 28.11.2018, p. 1–38).
[16] 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.

straight from the Regulation 2023/1543, not from the CCP – 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 the Regulation 2023/1543 are not compatible with the system used in the Polish CCP. However, they are compatible with the law of the EU and allow for the uniform use and application all across the EU MSs - 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 secondly, 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 MS in order to ensure effective application of the regulation, as, "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"[17].

III. Problem of equivalence and the Polish provisions in force

The 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

[17] See: E. Rotondo, *Is the EU's use of regulations becoming a trend?* (online).

not the population that moves, but services are placed in other countries than their users"[18]. On 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 then 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 MSs 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 (as in Preamble; motive 12). 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. There is a need to apply equivalent instruments regarding the obligations of both national and foreign providers. Actions taken on the basis of national law cannot lead to discrimination in relation to actions taken on the basis of EU regulation – especially when it comes to remedies enabling applying for damages[19]. 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.

Presently the Polish Code of Criminal Procedure 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 of the CCP as search and seizure) relates to the stage that can be an equivalent to a "production order". Secondly, the CCP introduces the obligation of service providers to secure certain digital data on the basis of a type of a "preservation order".

Article 236a CCP 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 CCP constitutes

[18] 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, *The European Legal Framework*, p. 251.
[19] 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.

the legal basis for production and preservation of IT data stored: 1) in an IT device; 2) in the IT system; 3) on a server; 4) on an information medium, including correspondence sent by e-mail. The provision applies both to the disposer and 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[20]. 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[21]. 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).

2/ seizure of evidence (Article 217). The method of seizure on the basis of Article 217 in connection with Article 236a CCP relates only to data in the IT system, not data from providers[22]. 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 connection with Article 236a CCP[23]). 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[24].

---

[20] J. Skorupka, in: *Kodeks postępowania karnego. Komentarz*, J, Skorupka (ed.), Warszawa 2023, p. 611.
[21] A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2003, vol. 10, p. 20; A. Lach, *Dowody elektroniczne w procesie*, p. 97.
[22] A. Lach, *Dowody elektroniczne w procesie*, p. 110; A. Lach, *Gromadzenie dowodów elektronicznych*, p. 22.
[23] A. Lach, *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, „Prokuratura i Prawo" 2005, vol. 10, p. 57
[24] A. Lach, *Gromadzenie dowodów elektronicznych*, p. 21

The scope of data that can be produced on the basis of the CCP provisions must be established. The Regulation 2023/1458 applies only to four types of stored data – which means that live communications are excluded. 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) - (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); computer assisted search[25]. 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 CCP are much wider: they relate to all data understood as a representation of facts or concepts communicated in a formalized way[26] and a medium is understood as any means of transporting data carrying any information[27]. Therefore, when deciding which provision would be applicable in the case of issuing a production order in the meaning of the Regulation, further procedural actions by the prosecutor or the court, will depend on the correct decision as to what specific data is involved. Later, the data from the provider may be seized (only in a limited scope, however) on the basis of Article 218 in connection with Article 236a CCP.

3/ seizure of data (Article 218, in the following scope resulting from Act of July 16, 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: 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 CCP in connection with Article 236a CCP, 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 CCP 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

[25] J. P. Mifsud Bonnici, M. Tudorica, J. A. Cannataci, *The European Legal Framework*, p. 216.
[26] Lach, *Dowody elektroniczne w procesie*, p. 20.
[27] P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, p. 46; W. Jasiński, *Pozyskiwanie informacji pochodzących z nośników danych dla celów postępowania karnego – węzłowe zagadnienia regulacji ustawowej*, „Gdańskie Studia Prawnicze" 2024, w druku.

"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 § 1-2 CCP[28]. Article 237 CCP is applied in connection with Article 241 CCP, that 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 connection with 241 CCP 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 email address) it is sufficient to apply Article 218 § 1 CCP. 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 § 1–2 CCP in connection with 241 CCP.

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 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 CCP applies also to "correspondence sent by e-mail". It means that Articles 217, 218 and 219 CCP can be applied

[28] See: J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, vol. 7-8, pp. 31-57.

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[29], 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[30]. 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 CCP), 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 a 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 (Article 236a and 241 CCP)[31]. It must be agreed that 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.

Article 218a CCP 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 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

[29] Lach, *Dowody elektroniczne w procesie*, p 33.
[30] See: J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola*, pp. 31-57.
[31] See: W. Jasiński, *Pozyskiwanie informacji pochodzących z nośników danych* (w druku).

authorities is very narrow. It is stipulated in Act of July 16, 2004 - Telecommunications Law, Articles 180c and 180d, and covers the same data as in the case of Article 218 in connection with Article 236a CCP. 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 CCP). In result, this provision applies both to content data and non-content data. Article 236a CCP (that applies only to the stage of production of evidence) does not apply to this provision, Article 218a CCP 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 CCP[32]. Thus, securing IT data is a kind of temporary measure preceding a possible request for their seizure (Article 217 § 1 in connection with Article 236a CCP). In order to carry out further activities, other legal grounds must be used.

On the basis of Article 218a CCP 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 CCP). 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[33]. At the same time seizure of these data – on the basis of Article 217 CCP – 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"[34]: According to Article 218a § 1 second sentence CCP, in cases of crimes specified in Article 200b (promoting pedophilia), Article 202 § 3, 4, 4a, 4b (public display of pornographic content) or Article 255a (dissemination of content that may facilitate the

[32] Lach, *Karnoprocesowe instrumenty zwalczania pedofilii*, p. 52–62.
[33] J. Skorupka, in: *Kodeks postępowania karnego. Komentarz*, (ed.) J. Skorupka, Warszawa 2023, s. 590.
[34] Article 218a § 1 amended by Article 3 point 2 letter a of the Act of April 20, 2021 (Journal of Laws 2021.1023) amending this Act as of June 22, 2021.

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, 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 effective application of the Regulation 2023/1458 it should be suggested that the 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. 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 of the Regulation 2023/1458 – 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"[35]. There is just one provisions – Article 218a CCP – adequately related to electronic evidence, but this is just a partial solution. In my opinion the Regulation, in order to be operational, requires better national legislation. Better than adopt "patches" to this chaotic model – a new structure for electronic evidence should be provided, suitable both for the needs of the 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 seize evidence by service providers. It should also give adequate powers to seize data available in open sources[36].

[35] W. Jasiński, *Pozyskiwanie informacji pochodzących z nośników danych* (w druku). Otherwise, wrongly: P. Opitek, *Przeszukanie na odległość jako czynność procesowa (Article 236a k.p.k.)*, „Prokuratura i Prawo" 2020, vol. 9, p. 126.

[36] See on the same topic: P. Lewulis, *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, „Prokuratura i Prawo" 2022, vol. 3, p. 144; W. Jasiński, Pozyskiwanie informacji pochodzących z nośników danych (w druku).

IV. The right to an effective remedy

Article 18 of the Regulation 2023/1543 provides for "effective remedies". First, any person whose data were requested via a European Production Order shall have the right to effective remedies against that order. Secondly, where that person is a suspect or an accused 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 this Article, 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 CCP). An interlocutory appeal is be provided against the decision on search and seizure (the "production order" based on Article 217 and 218 in connection with Article 236a CCP) and the decision on the basis of Article 218a CCP (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[37], arguing that Article 236 allows for an appeal against other actions relating to search, seizure of goods and physical evidence, but ignores securing them on the

[37] 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.

basis of Article 218a CCP (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 CCP[38]. It is necessary in the view of the obligation stemming from the Regulation 2023/1458 to provide a remedy to issuing an EPO. It can be derived from Article 236 CCP, however, it should be clearly stated, that also decision on issuing an EPO and EPrO, search and seizure of electronic evidence shocanuld be appealed[39]. Therefore, in this area another legislative change is needed.

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 CCP, 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 a EPO can use this provision to appeal that order – both suspects and other persons. Article 302 § 1 CCP 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[40]. It can be used then only when Article 236 § 1 CCP 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 CCP can be used – but only in the 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

[38] J. Skorupka, in: *Kodeks postępowania karnego. Komentarz*, (ed.) J. Skorupka, Warszawa 2023, p. 590.
[39] J. Grajewski, S. Steinborn, L.K. Paprzycki, *Kodeks postępowania karnego. Komentarz*, Warszawa 2013, p. 727.
[40] J. Grajewski, S. Steinborn, L.K. Paprzycki, *Kodeks postępowania karnego. Komentarz*, Warszawa 2013, p. 721. Zabłocki, *Postępowanie odwoławcze w nowym kodeksie postępowania karnego*, Warszawa 1997, p. 171; A. Jaskuła, *Zaskarżalność postanowień w przedmiocie dowodów rzeczowych*, „Prokuratura i Prawo" 2009, vol. 9, p. 38.

to use coercive methods; there is also no appeal against a decision not to introduce evidence. 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.

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 the 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))[41]. The national law in the case of the Polish CCP is located in Article 218 § 2 CCP (used in connection with Article 236a CCP) which states: "Delivery of the decision may be postponed for 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 connection with Art 241 CCP in relation to interception of communications, also in digital environment).

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 the 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 EU[42]. 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[43]. The effectiveness of the remedy should be evaluated on the basis of its effectiveness in the meaning of the Regulation 2023/1458.

V. The scope of control of the court

[41] 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, vol. 3, p. 193.
[42] OJ C 364/1, 8.12.2000.
[43] K. Lenaerts, *Trybunał Sprawiedliwości* Unii Europejskiej *a ochrona praw podstawowych*, „Europejski Przegląd Sądowy" 2013, vol. 1, p. 4-16.

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 the 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 a EPO to the private sector – placing on them "undue responsibility"[44]. 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 the Regulation 2023/1458. Therefore, it may be perceived as bypassing the MLA safeguards and the layers of fundamental rights scrutiny they entail[45]. 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 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 the 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

[44] V. Mitsilegas, *Editorial. The Privatisation of Mutual Trust in Europe's Area of Criminal Justice,* pp. 263–265.
[45] V. Mitsilegas, *Editorial. The Privatisation of Mutual Trust in Europe's Area of Criminal Justice*, pp. 263–265.

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 (Preamble, motive 33).

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:

- 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 execution 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. A European Production Order 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[46].

- 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 the EPO Regulation related to the risk that this law enforcement instrument may be abused to target journalists, human rights defenders, activists, political opponents and lawyers[47]. 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.

- 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 similar domestic case. The assessment of the adjudicating court should also take into account whether such EPO is limited to what was

[46] See: S. Tosza, *The E-Evidence Package is Adopted*, p. 167.
47 See: C. Berthélémy, *E-Evidence compromise blows a hole in fundamental*, "European Digital Rights" 2023, February, at: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/.

strictly necessary to achieve the legitimate aim of obtaining data that are relevant and necessary as evidence in an individual case.

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

In Article 17(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 European Production Order". Here it should be pointed out that in the Polish CCP, the defence has no real and effective opportunity either to get an EPO issued or to appeal this decision. Moreover, there is no procedure in which the defense could request that the evidence contained in the case-file be declared inadmissible. The defense can make a free (not regulated in the CCP) 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 and Directive (EU) 2016/680.

- 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 the Regulation 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 a 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 residing in Member States with systemic rule of law problems[48]. In

[48] C. Berthélémy, *E-Evidence compromise*, also see the scenarios and dangers elaborated 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.

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, that can object to the fulfilment of the EPO premises on every stage of criminal trial. With the direct route from the provider to the issuing MS's 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.

VI. 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. The Regulation 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 (motive 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".

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". This proposal, in accordance with information provided by the authors, "seeks to achieve the balance between

---

[66] *monstrating gaps in the e-Evidence Regulation*, "European Digital Rights" 2021, at: https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_10_20_EDRI_eEvidence%20Scenarios.pdf. See also on that topic: A. Juszczak, E. Sason, *The Use of Electronic Evidence*, p. 193.

defence safeguards and protection against crime 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"[49]. The proposal rightly observes that most legal systems of MSs 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[50].

The first stage of dealing with electronic evidence is forming them into evidence in a procedural sense. "Electronic evidence" that the Regulation 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[51]. During the negotiations over the Regulation it was suggested to replace the term with "a more neutral terminology", namely "electronic information"[52]. 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 trial. It should first of all decide, what is the proper form for such evidence. Then, there is a need to design a clear and functional method of preservation and presentation of electronic evidence as "evidence" in a procedural sense, as well as provide for the possibility to present such evidence by the parties in the court. Here, it is necessary to decide on what legal

[49] "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, at: https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-publishes-a-legislative-proposal-on-mutual-admissibility-of-evidence-and-electronic-evidence-in/

[50] 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, vol. 3, p. 226-227.

[51] 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*, Vanessa Franssen, Stanislaw Tosza (eds.), Cambridge University Press 2023, p. 9.

[52] 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)), Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Birgit Sippel, par. 147.

basis their admissibility should be evaluated. Finally, 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[53]. Therefore, taking into account the specificity of electronic (IT) data, which, along with other evidence, are the basis for making judgments, their evaluation must be extremely careful, because the life experience of every user of computer equipment shows that statistically these data are very often modified. However, it seems though that securing electronic evidence by service providers should lead 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).

VII. Conclusions

In the present state of law, Polish criminal procedure is not ready for the Regulation to operate. First, it lacks proper structure of gathering of electronic - and more generally digital – evidence. The state authorities have to move among a haze of contradicting 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 ensure effective application of the Regulation 2023/1458, 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. 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 the Regulation 2023/1458 – relies on "applying accordingly" "regular provisions" applicable in "real-life", analogue 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 the Regulation 2023/1458 and the production of electronic evidence from domestic service providers. There is a need to adopt a coherent standard for production of non-

[53] Decision of the Supreme Court of 20 June 2013, in the case no. III KK 12/13, published: LEX nr 1341691.

content and content data. Presently in the Polish CCP the standard to intercept electronic evidence of content data is much lower than in the EU law. 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. Of course, clear structure should not be understood as proposing wider access to such electronic data – only clear and predictable rules of such access[54]. This is an element of balancing between personal freedom and public security, which right now is regulated not only in national state orders but also by the EU. Lack of clear rules is an obstacle for the prosecutorial and judicial authorities which cannot use structured rules when deciding to reach for electronic (or wider: digital) evidence. One has to keep in mind the obligations for the national legislator resulting from the adoption of this form of EU legislation: national legislation must be provided that allows for effective execution of powers enshrined in the Regulation 2023/1458 as well as solutions that according to the Regulation belong to the area of legislation of national law.

Second, there is need of a 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

[54] On that see also: M. Jasiński, *Pozyskiwanie informacji pochodzących z nośników danych* (w druku), who 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".

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 the 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 MS. There is no specific regulation relating to this issue – as well as admissibility of electronic evidence. Therefore every MS 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 admissibility of electronic evidence[55]. Presently, Polish courts are left with the obligation – and freedom of assessment limited only by rules based on Article 7 CCP (taking into account the principles of correct reasoning and the recommendations of knowledge and life experience) – to assess the admissibility of electronic evidence, deciding on a case by case. So far, the Polish courts have only the existing legal system of admissibility of evidence – and speaking of a "system" is even a misuse of this notion. The only direction as to the rules of admissibility is Article 6 ECHR and the notion of fair trial and they should be applied also in EPO cases. Courts will generally basis.

There is no doubt that measures to obtain and preserve electronic evidence are increasingly important for criminal investigations and prosecutions across the Union. Regulation offers a breakthrough tool of cooperation, but it must be used thoroughly and in accordance with strict rules. 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[56]. It should give the national legislator the incentive to re-write the system of gathering and assessing applicability of

[55] See e.g. Request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 — Criminal proceedings against M.N., Case C-670/22, 2023/C 35/37; 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. …..

[56] See also on that topic: A. Juszczak, E. Sason, *The Use of Electronic Evidence*, p. 192-193.

electronic evidence. It is the highest time to deal with this issue in a coherent way, harmonized with the EU law.

References:

I/ Literature

1. Bachmaier L., *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings?,* "Eucrim" 2023, vol. 3;
2. Baldwin R., Cave M., Lodge M., *Regulation and the European Union*, in: *Understanding Regulation: Theory, Strategy, and Practice*, Baldwin R., Cave M., Lodge M. (eds.), Oxford University Press 2011;
3. Berthélémy C., *E-Evidence compromise blows a hole in fundamental*, "European Digital Rights" 2023, February, at: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/;
4. 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*, Franssen V., Tosza S. (eds.), Cambridge University Press 2023;
5. *Demonstrating gaps in the e-Evidence Regulation*, "European Digital Rights" 2021, at: https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_10_20_EDRI_eEvidence%20Scenarios.pdf;
6. Forlani G., *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, „Eucrim" 2023, vol. 3,
7. Grajewski J., Steinborn S., Paprzycki L.K., *Kodeks postępowania karnego. Komentarz*, Warszawa 2013;
8. Grzegorczyk T., Kodeks postępowania karnego. Komentarz, Warszawa 2014;
9. Hofmański P. (ed.), Sadzik E., Zgryzek K., Kodeks postępowania karnego. Komentarz, Warszawa 2007;
10. Jasiński W., *Pozyskiwanie informacji pochodzących z nośników danych dla celów postępowania karnego – węzłowe zagadnienia regulacji ustawowej*, „Gdańskie Studia Prawnicze" 2024, w druku.
11. Jaskuła A., *Zaskarżalność postanowień w przedmiocie dowodów rzeczowych*, „Prokuratura i Prawo" 2009, vol. 9;
12. 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, vol. 3;
13. Kornobis-Romanowska D., in: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom III*, A. Wróbel (ed.), Warszawa 2012;
14. Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, vol. 7-8;
15. Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004;
16. Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2003, vol. 10;
17. Lach A., *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, „Prokuratura i Prawo" 2005, vol. 10;

18. 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;
19. Lenaerts K., *Trybunał Sprawiedliwości* Unii Europejskiej *a ochrona praw podstawowych*, „Europejski Przegląd Sądowy" 2013, vol. 1;
20. Lewulis P., *Collecting Digital Evidence From Online Sources: Deficiencies In Current Polish Criminal Law*, "Criminal Law Forum" 2022, vol. 33;
21. Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021;
22. Lewulis P., *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, „Prokuratura i Prawo" 2022, vol. 3;
23. Mifsud Bonnici J. P., Tudorica M., Cannataci J. A., *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, in: Biasiotti M. A., Mifsud Bonnici J. P., Cannataci J., Turchi F. (eds.), *Handling and Exchanging Electronic Evidence Across Europe*, Springer 2018;
24. Mitsilegas V., *Editorial. 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);
25. Oerlemans J.J., van Toor D.A.G., *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, "European Journal of Crime, Criminal Law and Criminal Justice" 2022, vol. 30;
26. Opitek P., *Przeszukanie na odległość jako czynność procesowa (Article 236a k.p.k.)*, „Prokuratura i Prawo" 2020, vol. 9;
27. Pfeffer K., *Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln*, „Eucrim" 2023 vol. 3;
28. Rotondo E., *Is the EU's use of regulations becoming a trend*? Thomson Reuters Blog. 24/07/2013 at: http://publicsectorblog.practicallaw.com/is-the-eus-use-of-regulations-becoming-a-trend/;
29. Skorupka J., in: *Kodeks postępowania karnego. Komentarz*, J, Skorupka (ed.), Warszawa 2023;
30. 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;
31. 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);
32. 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. 2;
33. Tosza S., *The European Commission's Proposal on Cross-Border Access to E-Evidence*, "Eucrim" 2018, vol. 4;
34. Zabłocki S., *Postępowanie odwoławcze w nowym kodeksie postępowania karnego*, Warszawa 1997;

II/ Legal acts

1. Regulation (EU) 2023/1543 of the European Parliament and of the Council of the EU on European Production Orders and European Preservation Orders for electronic

evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, pp. 118–180.
2. 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 L 191, 28.7.2023, p. 181–190.
3. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 final.
4. Charter of Fundamental Rights of the EU OJ C 364/1, of 18.12.2000.
5. "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, at: https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-publishes-a-legislative-proposal-on-mutual-admissibility-of-evidence-and-electronic-evidence-in/
6. 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)), Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Birgit Sippel.

III/ Case law

1. ECJ judgment of 7 November 1972, case no. 20/72, NV Cobelex v Rechtbank van Koophandel Antwerpen, ECLI: ECLI:EU:C:1972:94;
2. ECHR judgment of 2 February 1977, case no. 5/76, Amsterdam Bulb BV v Produktschap voor Siergewassen, ECLI: ECLI:EU:C:1977:13.
3. ECJ judgment of 1 March 1973, case no. 40/69, Paul G. Bollmann Company and Hauptzollamt Hamburg-Waltershof, ECLI: ECLI:EU:C:1970:12.
4. ECJ judgment of 10 October 1973, in case 34/73, *Fratelli Variola S.p.A. and Amministrazione Italiana delle Finanze* ECLI: ECLI:EU:C:1973:101.
5. Decision of the Supreme Court of 20 June 2013, in the case no. III KK 12/13, published: LEX nr 1341691.
6. Request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 — Criminal proceedings against M.N., Case C-670/22, 2023/C 35/37.

The EU “E-Evidence package” from the Polish perspective: the highest time for a systemic change (iThenticate Smilarity Report)

ORIGINALITY REPORT

36%
SIMILARITY INDEX

PRIMARY SOURCES

1	www.europarl.europa.eu Internet	1369 words — 11%
2	eucrim.eu Internet	234 words — 2%
3	pure.mpg.de Internet	135 words — 1%
4	eur-lex.europa.eu Internet	121 words — 1%
5	orbilu.uni.lu Internet	104 words — 1%
6	hdl.handle.net Internet	103 words — 1%
7	publicsectorblog.practicallaw.com Internet	103 words — 1%
8	www.europeanlawinstitute.eu Internet	98 words — 1%
9	www.unodc.org Internet	83 words — 1%

10	europeanlawinstitute.eu Internet	81 words — 1%
11	link.springer.com Internet	63 words — < 1%
12	eurocoord.eu Internet	62 words — < 1%
13	journals.umcs.pl Internet	59 words — < 1%
14	edri.org Internet	50 words — < 1%
15	www.mpsp.mp.br Internet	49 words — < 1%
16	prawo.uni.wroc.pl Internet	47 words — < 1%
17	real.mtak.hu Internet	46 words — < 1%
18	curia.europa.eu Internet	45 words — < 1%
19	Radina Stoykova. "Digital evidence: Unaddressed threats to fairness and the presumption of innocence", Computer Law & Security Review, 2021 Crossref	42 words — < 1%
20	journals.ur.edu.pl Internet	42 words — < 1%
21	www.ibraspp.com.br Internet	

		41 words — < 1%
22	www.zrs-kp.si Internet	41 words — < 1%
23	www.researchgate.net Internet	39 words — < 1%
24	www.sip.lex.pl Internet	39 words — < 1%
25	euvalweb.euweb.org Internet	37 words — < 1%
26	research-portal.uu.nl Internet	37 words — < 1%
27	journals.sagepub.com Internet	36 words — < 1%
28	sic.pravo.upjs.sk Internet	35 words — < 1%
29	publications.cuni.cz Internet	34 words — < 1%
30	jssidoi.org Internet	33 words — < 1%
31	"The European Private Company - Societas Privata Europaea (SPE)", Walter de Gruyter GmbH, 2012 Crossref	31 words — < 1%
32	czasopisma.kul.pl Internet	30 words — < 1%

33	Stanislaw 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 Crossref	28 words — < 1%
34	www.casemine.com Internet	28 words — < 1%
35	www.cencenelec.eu Internet	28 words — < 1%
36	www.drugsandalcohol.ie Internet	28 words — < 1%
37	dokumen.pub Internet	27 words — < 1%
38	vdoc.pub Internet	27 words — < 1%
39	openaccess.uoc.edu Internet	25 words — < 1%
40	"European Investigation Order", Springer Science and Business Media LLC, 2023 Crossref	23 words — < 1%
41	Libor Klimek. "Mutual Recognition of Judicial Decisions in European Criminal Law", Springer Science and Business Media LLC, 2017 Crossref	23 words — < 1%
42	birgitsippel.de Internet	23 words — < 1%

43	libstore.ugent.be Internet	23 words — < 1%
44	trybunal.gov.pl Internet	22 words — < 1%
45	Valsamis Mitsilegas, Elena Fasoli, Fabio Giuffrida, Malgosia Fitzmaurice. "The Legal Regulation of Environmental Crime", Brill, 2022 Crossref	21 words — < 1%
46	emr-sb.de Internet	21 words — < 1%
47	www.lex-localis.press Internet	21 words — < 1%
48	bibliotekanauki.pl Internet	20 words — < 1%
49	tiptiktak.com Internet	20 words — < 1%
50	doczz.pl Internet	19 words — < 1%
51	ppuam.amu.edu.pl Internet	19 words — < 1%
52	ruj.uj.edu.pl Internet	19 words — < 1%
53	www.europol.europa.eu Internet	19 words — < 1%
54	www.informationpolicycentre.com Internet	18 words — < 1%

55	Foster, Nigel. "Blackstone's EU Treaties & Legislation", Blackstone's EU Treaties & Legislation, 2023 Publications	17 words — < 1%
56	ebin.pub Internet	17 words — < 1%
57	www.eumonitor.eu Internet	17 words — < 1%
58	www.fedtrust.co.uk Internet	17 words — < 1%
59	www.kssip.gov.pl Internet	17 words — < 1%
60	docplayer.pl Internet	16 words — < 1%
61	media.frag-den-staat.de Internet	16 words — < 1%
62	www.gesetze-im-internet.de Internet	16 words — < 1%
63	www.rug.nl Internet	16 words — < 1%
64	www.uwm.edu.pl Internet	16 words — < 1%
65	"Judicial Protection in Transnational Criminal Proceedings", Springer Science and Business Media LLC, 2021 Crossref	15 words — < 1%

66	intellectdiscover.com Internet	15 words — < 1%
67	sei.iuridica.truni.sk Internet	15 words — < 1%
68	www.gov.pl Internet	15 words — < 1%
69	kryminalistyka.wpia.uw.edu.pl Internet	14 words — < 1%
70	www.scribd.com Internet	14 words — < 1%
71	Maciej Rogalski. "The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes", European Journal of Crime, Criminal Law and Criminal Justice, 2020 Crossref	13 words — < 1%
72	quieora.ink Internet	13 words — < 1%
73	Fran Casino, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, Constantinos Patsakis. "SoK: cross-border criminal investigations and digital evidence", Journal of Cybersecurity, 2022 Crossref	12 words — < 1%
74	depotuw.ceon.pl Internet	12 words — < 1%
75	library.oapen.org Internet	12 words — < 1%
76	research.ou.nl	

Internet

12 words — < 1%

77 Izabela Urbaniak-Mastalerz. "Application of the Provisions of the Code of Criminal Procedure in Disciplinary Proceedings Against Attorneys", Białostockie Studia Prawnicze, 2017
Crossref

11 words — < 1%

78 www.bibliotekacyfrowa.pl
Internet

11 words — < 1%

79 Alina Kaczorowska-Ireland. "European Union Law", Routledge, 2016
Publications

10 words — < 1%

80 Quynh Anh Tran. "Chapter 10 Using Electronic Evidence in Civil and Commercial Dispute Resolution: Challenges and Opportunities", Springer Science and Business Media LLC, 2022
Crossref

10 words — < 1%

81 assets.gov.ie
Internet

10 words — < 1%

82 pdffox.com
Internet

10 words — < 1%

83 Jeffrey Kenner. "European Union Legislation", Routledge, 2012
Publications

9 words — < 1%

84 Paul de Hert, Cihan Parlar, Juraj Sajfert. "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law", Computer Law & Security Review, 2018
Crossref

9 words — < 1%

85	Piotr Krzysztof Sowiński. "Formation of Some Elements of the Right to Defence in Misdemeanour Proceedings", Ius Novum, 2024 Crossref	9 words — < 1%
86	e-revistas.uc3m.es Internet	9 words — < 1%
87	pure.uvt.nl Internet	9 words — < 1%
88	www.cybercrime.umk.pl Internet	9 words — < 1%
89	www.hraction.org Internet	9 words — < 1%
90	www.legislation.gov.uk Internet	9 words — < 1%
91	"European Citizenship under Stress", Brill, 2020 Crossref	8 words — < 1%
92	"Handling and Exchanging Electronic Evidence Across Europe", Springer Science and Business Media LLC, 2018 Crossref	8 words — < 1%
93	Hanna Kuczyńska. "Admissibility of Evidence Obtained as a Result of Issuing an European Investigation Order in a Polish Criminal Trial", Review of European and Comparative Law, 2021 Crossref	8 words — < 1%
94	Hanna Kuczyńska. "The Accusation Model Before the International Criminal Court", Springer Nature, 2015	8 words — < 1%

Crossref

95	curis.ku.dk Internet	8 words — < 1%
96	era-comm.eu Internet	8 words — < 1%
97	export.arxiv.org Internet	8 words — < 1%
98	lauda.ulapland.fi Internet	8 words — < 1%
99	www.coe.int Internet	8 words — < 1%
100	www.parlament.gv.at Internet	8 words — < 1%
101	www.statewatch.org Internet	8 words — < 1%
102	wydawnictwo.uwm.edu.pl Internet	8 words — < 1%
103	Alina Kaczorowska-Ireland. "European Union Law", Routledge, 2019 Publications	7 words — < 1%
104	Filip Radoniewicz. "Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego", Cybersecurity and Law, 2022 Crossref	7 words — < 1%
105	Quynh Anh Tran. "Chapter 8 The Admission of Electronic Evidence in Civil and Arbitral	7 words — < 1%

Proceedings", Springer Science and Business Media LLC, 2022
Crossref

106 "The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings", Springer Science and Business Media LLC, 2020 — 6 words — < 1%
Crossref

107 Alina Kaczorowska-Ireland. "European Union Law", Routledge-Cavendish, 2019 — 6 words — < 1%
Publications

108 Christie, Andrew. "Blackstone's Statutes on Intellectual Property", Blackstone's Statutes on Intellectual Property, 2023 — 6 words — < 1%
Publications

109 Jacek Barcik. "Wielopoziomowy konstytucjonalizm Unii Europejskiej a stosowanie praw podstawowych", Przegląd europejski, 2019 — 6 words — < 1%
Crossref

110 John P. Grant, J. Craig Barker. "International Criminal Law Deskbook", Cavendish Publishing (Australia) Pty Ltd, 2013 — 6 words — < 1%
Publications

111 Karlik, Piotr and Wiliński, Paweł(Karlik, Piotr and Wiliński, Paweł). "Improving protection of victims' rights: access to lega aid", Repozytorium Uniwersytetu im Adama Mickiewicza AMUR, 2014. — 6 words — < 1%
Publications

112 Marcin Wielec, Tomasz Bojanowski. "Przesłuchanie świadka w procesie karnym w trybie art. 185e Kodeksu postępowania karnego", Prawo w Działaniu, 2024 — 6 words — < 1%
Crossref

113	Monika Nowikowska. "Procesowa kontrola danych informatycznych w chmurze obliczeniowej", Cybersecurity and Law, 2023 Crossref	6 words — < 1%
114	Richard Bellamy. "The Rule of Law and the Separation of Powers", Routledge, 2017 Publications	6 words — < 1%
115	aei.pitt.edu Internet	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF