sciendo

Ius Novum

2023, vol. 17, no. 4, pp. 1–14

THE CONCEPT OF EVIDENCE OBTAINED FROM ELECTRONIC CORRESPONDENCE

MACIEJ ROGALSKI*

DOI: 10.2478/in-2023-0026

Abstract

This article addresses cross-border cooperation between Polish law enforcement authorities and those of other European Union Member States in obtaining electronic evidence in criminal matters. It discusses provisions such as Article 589g § 1, Article 589l § 1, Article 589w § 4, and Article 589ze § 10 of the Code of Criminal Procedure (CCP), focusing on defining electronic evidence. Currently, there are no legal definitions for these terms. The article posits that the existing definitions of electronic evidence are imprecise and lead to interpretational doubts. Therefore, it is crucial to organise the conceptual framework in the CCP by creating new definitions or clarifying existing ones. The analysis incorporates the provisions of Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and the execution of custodial sentences following criminal proceedings.

Keywords: electronic evidence, correspondence, telephone call lists, information transmissions, data

INTRODUCTION

The international cooperation between Polish law enforcement bodies and those of other European Union Member States in obtaining electronic evidence is governed by Chapters 62a–d of the Act of 6 June 1997: Code of Criminal Procedure.[1] Provisions in Chapters 62a and 62b CCP cover requests to an EU Member State to execute a decision to seize evidence and requests by an EU Member State for execution

* Professor, LLD hab., Faculty of Law and Administration, Lazarski University (Poland), e-mail: maciej@rogalski.waw.pl, ORCID: 0000-0003-4366-642X.

1 Consolidated text, Journal of Laws of 2022, item 1375, as amended, hereinafter 'CCP'.

of a ruling to seize evidence. Chapters 62c and 62d CCP deal with requests to an EU Member State to conduct investigative measures under the European Investigation Order (EIO)[2] and requests by an EU Member State to conduct such measures.

Article 589g § 1 CCP states that if items, correspondence, postal materials, telephone call lists, or other information or data transmissions stored in computer systems or on data carriers, including electronic correspondence, may constitute evidence in criminal matters and are within the territory of an EU Member State, a competent court or prosecutor can directly request a judicial body of that State to execute a decision to seize or preserve them. Article 589l §§ 1–2 CCP sets out a similar regulation for the execution by a competent regional court or prosecutor of a ruling issued by a judicial body of another EU Member State to seize such items.

Article 589w § 4 CCP addresses the provision of electronic evidence at the request of a Polish court or prosecutor under the EIO.[3] This regulation pertains to issuing an EIO to control and record telephone conversations and other conversations or information transmissions, including electronic correspondence, using technical means. Article 589ze § 10 CCP provides analogous provisions for applications from another EU Member State to a Polish court or prosecutor under the EIO.

Articles 589g § 1, 589l § 1, 589w § 4, and 589ze § 10 CCP use terms related to electronic evidence but they lack legal definitions. This article aims to define those terms. It argues that current definitions of electronic evidence are imprecise and raise interpretational doubts; thus, it is necessary to organise the conceptual framework used in the provisions regulating international cooperation in criminal matters between EU Member States. This requires developing definitions that clarify the terms used in the context of evidence obtained from electronic communication. The analysis is taking into account provisions of the newly adopted Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and the execution of custodial sentences following criminal proceedings (hereinafter 'Regulation 2023/1543').[4]

ELECTRONIC EVIDENCE

At the outset, it is important to note that neither the Code of Criminal Procedure nor the Criminal Code[5] contains a legal definition of 'electronic evidence'. In legal doctrine, 'electronic evidence' refers to various types of evidence, particularly data

---

[2] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1), hereinafter 'EIO'.

[3] In practice the EIO is used more and more often, see Klimczak, J., Wzorek, D., Zielińska, E., *Europejski nakaz dochodzeniowy w praktyce sądowej i prokuratorskiej – ujawnione problemy i perspektywy rozwoju*, Warszawa, 2022, pp. 100–104.

[4] OJ L 191, 28.7.2023, p. 118.

[5] Act of 6 June 1997: Criminal Code, consolidated text, Journal of Laws of 2022, item 1138, as amended, hereinafter 'CC'.

collected in computer systems or obtained during correspondence interception or through recording information on data carriers. It is also noted that electronic evidence includes information and data in digital form, as well as information stored or transmitted in binary form.[6]

According to the Budapest Convention, electronic evidence refers to evidence of a criminal offence that can be collected electronically.[7] Article 3(8) of Regulation 2023/1543 defines 'electronic evidence' as '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 (EPOC) or a European Preservation Order Certificate (EPOC-PR)'. This definition includes several terms also defined in Regulation 2023/1543: 'subscriber data' (Article 3(9)), 'traffic data' (Article 3(11)), 'content data' (Article 3(12)), and 'service provider' (Article 3(3)).

The CCP in its provisions on international cooperation between EU Member States in criminal matters, refers to electronic evidence as:

– correspondence, postal items, telephone call lists, or other information or data transmissions stored in computer systems or on data carriers, including electronic correspondence (Article 589g § 1 CCP; Article 589l § 1 CCP);
– controlling and recording the content of telephone conversations and recording other conversations or information transmissions using technical means, including email correspondence (Article 589w § 4 CCP; Article 589l § 1 CCP).

Given the subject and purpose of this article, it is necessary to attempt to define the terms used in these provisions to refer to electronic evidence. Regulation 2023/1543 is particularly helpful in determining the general concept of 'electronic evidence', as it contains such a definition. Adopting the definition of electronic evidence from EU Regulation 2023/1543 highlights its differences and specificity compared to other evidence, and underscores its practical importance. Recitals 6, 8, 9, 27, 31, 40, and 41 of the preamble to Regulation 2023/1543 underline the significance of electronic evidence and international cooperation in obtaining it. Particularly, recital 31 clarifies the scope of data covered by Regulation 2023/1543 and thus forms the basis of the definition of 'electronic evidence' within this Regulation. It categorises data into subscriber data, traffic data, and content data. Next, it explains that: 'Such categorisation is in line with the law of many Member States and Union law, such as Directive 2002/58/EC and the case law of the Court of Justice, as well as international law, in particular the Budapest Convention.'

As Regulation 2023/1543 is a Union Regulation, all Member States are obliged to apply its provisions, including the definition of 'electronic evidence'. Given the

---

[6] Lach, A., *Dowody elektroniczne w procesie karnym*, Toruń, 2004, pp. 29–67; Adamski, A., *Prawo karne komputerowe*, Warszawa, 2000, p. 192 et seq.; Oręziak, B., 'Dowody elektroniczne a sprawiedliwość procesu karnego', *Prawo w Działaniu*, 2020, No. 41, p. 191; Cassey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Baltimore, 2000, p. 93 et seq.; Lambert, P., 'The Search for Elusive Electrons: Getting a Sense of Electronic Evidence', *Judicial Studies Institute Journal*, 2001, No. 1, pp. 24–27; Taylor, M., Haggerty, J., Gresty, D., Hegarty, R., 'Digital evidence in cloud computing systems', *Computer Law & Security Review*, 2010, No. 3, pp. 306–307.

[7] Council of Europe Convention on Cybercrime (ETS No 185), done at Budapest on 23 November 2001, Journal of Laws of 2015, item 728.

absence of a general definition of electronic evidence in Chapters 62a–62d CCP and the need to align them with Regulation 2023/1543, introducing this definition into the national provisions would be justifiable.

CORRESPONDENCE, INCLUDING CORRESPONDENCE SENT BY EMAIL

The provisions of Article 589g § 1 CCP and Article 589l § 1 CCP use the term 'przesyłka' ['post'], which may lead to interpretational doubts, particularly concerning the scope of electronic evidence. The Act: Postal Law[8] does not define '*przesyłka*' but does define '*przesyłka pocztowa*' [literally 'postal post', i.e. an item sent and delivered by post]. Under Article 3(21) PL, *przesyłka pocztowa* is a postal item with an addressee's designation and address, submitted to or received by a postal operator for transport and delivery. Given the traditional physical delivery of post, a postal item in this sense cannot be considered electronic evidence. Despite the imprecise use of the adjective '*pocztowy*', the noun '*przesyłka*' seems to be used in this context in Article 218 § 1 CCP, as the provision mandates post offices and entities providing postal services to distribute postal items. Thus, it should be assumed that the term '*przesyłka*' in Article 589g § 1 CCP and Article 589l § 1 CCP does not pertain to evidence obtained from electronic communication.

The term 'correspondence' raises doubts and requires clarification. It is generally understood to mean the method of communication between people (both natural and legal persons) in any form, particularly in writing, orally, via pictures, or any other means, e.g., through written post, fax, telegraph, telephone (including SMS and MMS), electronic mail (email), etc.[9] In legal doctrine, two concepts are distinguished based on the form of communication: correspondence in the broad sense (*sensu largo*), covering all forms of communication between people, not just in writing but also through other means; and correspondence in the narrow sense (*sensu stricto*), which includes only written communication.[10] For the purposes of this article, the broader meaning of 'correspondence' should be adopted, encompassing all forms of communication, not limited to writing (letters, postal items) but also including other means such as telephone, radio, fax, telegraph, internet, and all modern telecommunication developments.[11]

---

[8] Act of 23 November 2012: Postal Law, consolidated text, Journal of Laws of 2022, item 896, as amended, hereinafter 'PL'.

[9] Ferenc-Szydełko, E., *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Legalis 2014, part I, subsection 1 to Article 82.

[10] Cf. Taras, T., 'O dopuszczalności i legalności podsłuchu telefonicznego', *Annales UMCS*, section G, Lublin, 1960, p. 51; Dudka, K., 'Zatrzymanie korespondencji w projekcie kodeksu postępowania karnego z 1995 r. na tle przepisów obowiązujących', *Prokuratura i Prawo*, 1996, No. 4, p. 11; Dudka, K., *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin, 1998, pp. 11–12.

[11] Kunicka-Michalska, B., 'Przestępstwa przeciwko ochronie informacji', in: Wąsek, A. (ed.), *Kodeks karny*, Vol. II, Warszawa, 2010, p. 928; Rogalski, M., *Kontrola korespondencji*, Warszawa, 2016, pp. 19–20. Also see Hofmański, P., 'Komentarz do wybranych przepisów Europejskiej

Defining the term 'correspondence' more precisely with the use of the phrase 'including correspondence sent by electronic mail' does not seem to require additional explanation, as the term 'electronic mail' is commonly used. The specification phrase 'including correspondence sent by electronic mail' used in the provisions is also in conformity with the concept of correspondence *sensu largo*. Even though this kind of specification does not fully clarify whether it pertains to the content of correspondence or merely the fact of its occurrence, such as the action of sending an email. Regulation 2023/1543 categorises data into two primary types: traffic data and content data. To avoid interpretational ambiguities, it is suggested to replace the term 'correspondence' with these two concepts, depending on whether the focus is on the occurrence of correspondence or its content.

LISTS OF TELEPHONE CALLS OR OTHER TRANSMISSIONS OF INFORMATION

The term 'telephone call list' poses the fewest interpretational challenges. It should be understood that 'lists of calls', as used in Article 589g § 1 CCP and Article 589l § 1 CCP, refer to data outlined in Articles 180c and 180d of the Telecommunications Law.[12] Based on Article 180c(2) of this law, the Minister of Infrastructure issued the Regulation of 28 December 2009 on detailed lists of data and types of operators of public telecommunications networks or providers of publicly available telecommunications services obliged to seize and store them was issued.[13] The Regulation in particular details data necessary for: (1) identifying the network end, the telecommunications end device, and the end user who initiates a call; (2) identifying the network end, the telecommunications end device, and the end user receiving the call; (3) establishing the date, time, and duration of a call; (4) categorising call types; (5) determining the location of the telecommunications end device (§ 1 of the Regulation of 28 December 2009).

According to the Regulation of 28 December 2009, for services within the land-line public telecommunications network, the first and second groups of data seized by an entrepreneur include: the number of the network end for both the initiating and receiving subscribers, their first names, surnames or names, and addresses. For mobile network services, data include the MSISDN of the calling and called subscribers,[14] first names, surnames or names, and addresses if available, the user's

---

Konwencji o ochronie praw człowieka i podstawowych wolności', in: Zielińska, E. (ed.), *Standardy Prawne Rady Europy. Teksty i komentarze. Tom III, Prawo karne*, Warszawa, 1995, p. 99.

[12] Act of 16 July 2004: Telecommunications Law, consolidated text, Journal of Laws of 2022, item 1648, as amended, hereinafter 'TL'.

[13] Journal of Laws of 2009, No. 226, item 1828, hereinafter 'Regulation of 28 December 2009'.

[14] The abbreviation MSISDN stands for Mobile Station International Subscriber Directory Number. It means a number of a mobile network subscriber, commonly known as a telephone number.

IMSI,[15] the first 14 digits of the IMEI number[16] or the ESN.[17] For pre-paid service users, additional data include the date and time of the first telecommunications log-in of the end device to the mobile network, local time, and the geographical coordinates of the mobile network station (BTS)[18] used for logging in. For internet, email, and internet telephony services, data comprise the user's identification number, dial-up access number, IP address,[19] first name, surname or name, and address of the end user assigned the IP address during the call, as well as the identification number or the Internet telephone service number assigned to them, the identification number of the network end used for internet access, especially the identification number of the digital subscriber line DSL,[20] the network port number used, or the MAC address of the end device. In the case of email and internet telephone services, subscriber data are limited to the internet telephone number, first name, surname or name, and address of the registered end user of the email or internet telephone service, and their identification number (§ 3(1)–(2), § 4(1)–(2), § 6(1), § 7(1) of the Regulation of 28 December 2009).

The third group of data includes the date and time of a call and its duration. For both landline and mobile networks, it is necessary to establish the date and time of a failed attempt to connect or of the connection establishment and termination, according to local time, as well as the call duration with one-second accuracy. For Internet access services, the date and time of every connection and disconnection to the Internet, including the assigned dynamic and static IP addresses used during the connection and the user's identification number, are recorded (§ 3(3), § 4(3), § 6(2) of the Regulation of 28 December 2009).

The fourth type of data pertains to the type of connection. For services provided via both landline and mobile networks, as well as electronic mail and internet telephone services, the type of service used is established, e.g., voice call (§ 3(4), § 4(4), § 6(2), § 7(2) of the Regulation of 28 December 2009).

The last group of data concerns the positioning of the end device. In landline networks, the address of the location of the telecommunication end device is established. In mobile networks, for devices within the territory of Poland, the identification number of the BTS antenna during the connection or the start of reception, geographical coordinates of the BTS in the area where

---

15 The abbreviation IMSI stands for International Mobile Subscriber Identity and means a unique number of every SIM card in the cellular telecommunication network and identifying it. In turn, the SIM card (Subscriber Identity Module) means a module identifying a subscriber, in the form of a plastic chip card with embedded memory and a microprocessor.

16 IMEI (International Mobile Equipment Identity) means an individual numeric identifier of a mobile phone, which may be displayed on screen on every phone by entering the code *#06#.

17 The abbreviation ESN means Electronic Serial Number, which is a unique 32-bit identification number assigned to mobile phones by their producers. The ESN is embedded in the telephone microprocessor.

18 The abbreviation BTS (Base Transceiver Station) means a transceiver station in the wireless communication systems.

19 IP (Internet Protocol) means the basic protocol used on the Internet.

20 DSL (Digital Subscriber Line) means a digital subscriber line/loop, a digital technology for wide-band access to the Internet.

the telecommunications end device was located, and the azimuth, beam and working range of the BTS antenna are recorded. For devices outside the territory of Poland, the MCC identification (country number) and the mobile network code (MNC) of the initiating and receiving call are established.

Apart from lists of telecommunications connections, regulations also provide for lists of other information transmissions. These refer to data transmissions other than telecommunications connections and concern the transmission of information, e.g., lists of sent short messages or the transmission of a particular amount of data. More information on this can be found in the part of the article devoted to 'Content of other conversations or transmissions of information'.

The content of 'a list of telephone calls' and 'other transmissions of information' aligns with the concept of 'traffic data' as defined in Article 3(11) of Regulation 2023/1543. This means

> 'data related to the provision of a service offered by a service provider which serve to provide context or additional information about such service and are generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, the location of the device, date, time, duration, size, route, format, the protocol used, the type of compression, and other communications metadata and data, other than subscriber data, relating to the commencement and termination of a user access session to a service, such as the date and time of use, the log-in and log-off from the service.'

To avoid terminological discrepancies and practical difficulties in applying different terms, it will be necessary to standardise concepts. In this case it will be necessary to replace the terms 'list of telephone calls' and 'other transmissions of information' with 'traffic data'.

It should also be noted that Articles 180c to 180d of the Telecommunications Law result from implementing Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.[21] The provisions of this Directive were implemented to Polish law through an amendment to the Telecommunications Law of 24 April 2009.[22] However, in the *Digital Rights Ireland* case, the Court of Justice of the EU (hereinafter CJEU) declared this Directive invalid.[23] The judgement of the CJEU binds all courts and bodies of EU Member States.[24] The Polish Constitutional Tribunal, in its judgement of 30 July

---

[21] OJ L 105, 13.4.2006, p. 54, hereinafter 'Directive 2006/24/EC'.

[22] Act amending Act: Telecommunications Law and some other acts, Journal of Laws of 2009, No. 85, item 716.

[23] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[24] Cf. Szpunar, M., in: Kornobis-Romanowska, D., Łacny, J., Wróbel, A. (eds), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, Vol. III, Warszawa, 2012, commentary on Article 267 TFEU, subsection 267.9.2.

2014, also stated that the CJEU's judgement binds not only EU institutions and bodies but also all authorities of EU Member States, including courts.[25]

Although Directive 2006/24 was declared invalid, there were legal grounds for the retention of data laid down in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).[26] However the CJEU issued successive judgements, which concerned this Directive as grounds for creating national provisions in the field of communications data retention. The CJEU stated in its judgement of 21 December 2016 in the *Tele2 Sverige AB v Post-och telestyrelsen* case that Article 15 of the Directive 2002/58/EC puts obstacles in the way of national regulations, 'which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.'[27] The CJEU expressed a similar view in its judgement of 5 April 2022 in the *G.D. v The Commissioner of the Garda Síochána and Others* case.[28]

Despite the aforementioned judgements, Articles 180c to 180d TL have remained largely unchanged. Doubts have been raised about the appropriateness of the regulation concerning telecommunications data retention.[29] The current provisions of Articles 180c and 180d TL are general and do not differentiate in terms of the scope and type of collected data. They permit storing all traffic and location data of all subscribers and registered users of electronic communication means and do not restrict data access solely to serious crime fighting purposes. Consequently, these provisions may be in conflict with Articles 7, 8, and 52(1) of the Charter of Fundamental Rights of the European Union.[30] In legal doctrine, it is noted that the legislator's inaction in amending data retention regulations in Poland may have legal repercussions, affecting not only ongoing criminal proceedings but also concluded ones. This concern pertains to domestic criminal cases adjudicated in recent years where data retained under national provisions served as the basis for conviction.[31]

The implementation of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code[32] into Polish law necessitated drafting of a new legal act:

---

[25] See the judgement of the Constitutional Tribunal of 30 July 2014, K 23/11, *Orzecznictwo Trybunału Konstytucyjnego*, A 2014, No. 7, item 80, subsection 10.4.4. of the justification.

[26] OJ L 201, 31.7.2002, p. 37, hereinafter 'Directive 2002/58/EC'.

[27] Case C-203/15, ECLI:EU:C:2016:970.

[28] Case C-140/20, ECLI:EU:C:2022:258.

[29] See Brzeziński, P., 'Glosa do wyroku Trybunału Sprawiedliwości z dnia 21 grudnia 2016 roku w sprawach połączonych C-203/15 I C-698/15', in: Opaliński, B. and Rogalski, M. (eds), *Kontrola korespondencji. Zagadnienia wybrane*, Warszawa, 2018, pp. 76–84; Rogalski, M., 'Are the Regulations with Respect to the Retention and Provision of Communications Data Appropriate in Poland? A Proposal for Changes', *Ius Novum*, 2015, No. 2, pp. 229–231.

[30] Consolidated text, OJ C 202, 7.6.2016, hereinafter 'CFR'.

[31] For more, see Rojszczyk, M., 'Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna', *Państwo i Prawo*, 2023, No. 2, pp. 46–55.

[32] OJ L 321, 17.12.2018, p. 36.

the Electronic Communications Law ('ECL').[33] Although initially scheduled to come into force in the first half of 2024, the bill was subsequently withdrawn from the Sejm's proceedings. The bill provisions concerned not only telecommunications entrepreneurs and the provision of telecommunications services but also electronic communication companies and the provision of electronic communication and interpersonal communication services. However, the type, scope, and method of collecting telecommunications data remained unchanged. The new provision of Article 49(1) ECL, concerning telecommunications data, essentially mirrored Article 180c(1) TL. Hence, the regulation of telecommunications data subject to retention and available to authorised entities remains a current issue. The provisions of Articles 180c and 180d of the existing Telecommunications Law are, in light of Union judgments, in conflict with the Charter of Fundamental Rights of the European Union. The ECL, in its current form, fails to address this issue, as the content of the new regulations (Article 49(1) ECL) merely replicates the old, currently binding ones (Articles 180c and 180d TL). The only solution seems to lie in revising Article 49 to align with the guidelines laid down in the CJEU judgements. This would entail a more nuanced approach to data retention conditions not generic in nature. Instead of uniformly applying the same criteria to all data types, the approach and conditions for retention should vary according to the specific type of data subject to retention.

DATA STORED IN COMPUTER SYSTEMS OR ON DATA CARRIERS

The term 'data' in Polish criminal law has various meanings. Article 218 § 1 CCP refers to 'the data mentioned in Articles 180c and 180d' TL.[34] Meanwhile, Article 20c (1)(1) of the Act of 6 April 1990 on the Police[35] refers to these as 'telecommunications data'. Articles 218a § 1 and 236a of the CCP use the term 'computer data', as does Article 268a § 1 CC.[36] According to Article 1(b) of the Council of Europe Convention on Cybercrime (Budapest Convention, 23 November 2001), 'computer data' means 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'.[37]

Article 236a of the CCP mentions 'data stored in a computer system or on a carrier', referring to computer data in the possession of the system holder or user.

---

[33] The Sejm print No. 2861 of 9 December 2022, hereinafter 'ECL', https://orka.sejm.gov.pl/Druki9ka.nsf/0/24242EFE9A7B0D08C12589170036022D/%24File/2861.pdf, accessed on 4 May 2023.

[34] The present content of Article 218 CCP is the consequence of the amendment to CCP introduced several years ago resulting from the implementation of Directive 2006/24/EC (Act of 24 April 2009 amending Act: Telecommunications Law and some other acts, Journal of Laws of 2009, No. 85, item 716).

[35] Consolidated text, Journal of Laws of 2023, item 171, as amended, hereinafter 'AP'.

[36] Act of 6 June 1997: Criminal Code, consolidated text, Journal of Laws of 2022, item 1138, as amended, hereinafter 'CC'.

[37] Journal of Laws of 2015, item 728, hereinafter 'the Budapest Convention'.

This term employs the concept of a computer system, which, as per Article 1(a) of the Budapest Convention, is 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data'.

It is important to note that the Budapest Convention identifies three categories of data: the aforementioned 'computer data'; 'traffic data', defined as any computer data relating to a communication by means of a computer system, generated by a system that forms part of the communication chain, indicating the communication origin, destination, route, time, date, size, duration, or type of underlying service (Article 1(d) of the Budapest Convention); and 'intercepted content data', subject to transmission using technical means (Article 21 of the Budapest Convention).

Besides the aforementioned concepts, the term 'Internet data' is also used in Polish law. The Act of 18 July 2002 on the provision of electronic services,[38] allows for the collection of data necessary to provide electronic services (Article 18(1)–(5) of this Act). According to Article 18(5) of the Act on the Provision of Electronic Services (APES), a service provider may process the following exploitation data characterising the use of electronic services by a user: identifiers of the service user (Article 18(1) APES); identifiers of the telecommunications network end or the information and communication technology system used by the service user; information about the commencement, termination, and scope of each use of the service provided electronically. Article 20c(1)(3) of the Act calls these data 'Internet data'. Additionally, the term 'postal data' refers to data mentioned in Article 82(1)(1) PL, as per Article 20c(1)(2) of the AP. However, these data are not electronic in nature.

Articles 589g § 1 and 589l § 1 of the Code of Criminal Procedure (CCP) refer to data stored in a computer system or on a carrier. The term 'data in a computer system', as defined in the Budapest Convention, is used. However, there is no mention of storing data in devices, thus the provisions do not refer to data stored in information system devices. Data can be stored on carriers such as external discs or pen drives. There are various methods for data retention.[39]

The concept of 'data stored in a computer system or on a carrier' aligns with the definition of 'content data' in Article 3(12) of Regulation 2023/1543 and the term 'information system' defined in Article 3(13). 'Content data' refers to 'any data in digital format, such as text, voice, videos, images, and sound, other than subscriber data or traffic data'. 'Information system' refers to an information system as defined in Article 2(a), of Directive 2013/40/EU of the European Parliament and of the Council.[40] Similarly, in the case of these terms, due to the fact that Regulation 2023/1543 is binding, in order to avoid terminological discrepancies, it will be necessary to replace the term 'data stored in a computer system or on a carrier' with the term 'content data'.

---

[38] Consolidated text, Journal of Laws of 2020, item 344, as amended, hereinafter 'APES'.

[39] See Szumiło-Kulczycka, D., in: Skorupka, J. (ed.), *System prawa karnego procesowego. Dowody*, Vol. VIII, part 3, Warszawa, 2019, pp. 3255, 3257.

[40] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8.

CONTENT OF OTHER CONVERSATIONS OR TRANSMISSIONS OF INFORMATION

Articles 589w § 4 and 589l § 1 of the CCP provide for 'controlling and recording the content of telephone conversations and recording the content of other conversations or transmissions of information using technical means'. The term 'telephone conversations' is self-explanatory. However, the phrase 'the content of other conversations or transmissions of information' raises interpretational doubts.[41]

It should be assumed that 'the content of other telephone conversations and transmissions of information', as defined in Article 2(42) of the Telecommunications Law (TL), covers all transmissions of information in telecommunications, regardless of their type, using cables, radio, optical waves, or other means employing electromagnetic energy, e.g., on the Internet.[42] The concept of information transmission encompasses a transfer that involves information shared by users of telecommunications services. As per Article 2(27a) TL, telecommunications transmission means the content of telephone conversations and other information transmitted using telecommunications networks, e.g., emails or text messages.

This definition of telecommunications transmission was added in the amendment to the Telecommunications Law of 24 April 2009, pertaining to the powers of courts, prosecutors, or authorised entities to access and record the content of information transmitted in telecommunications networks. It is correctly emphasised that the phrase referring to information transmitted using telecommunications networks is a fundamental element defining telecommunications transmission. A telephone conversation is merely an example of possible transmission content. As a result of this definition, telecommunications transmission encompasses all information transmitted in telecommunications networks.[43]

It should be assumed that other conversations or information transmissions also include conversations or transmissions of information outside telecommunications networks[44] within the meaning of Article 2(35) TL. Other conversations refer to those not conducted using telecommunications devices, as defined in Article 2(46) TL. Therefore, these include conversations occurring indoors or outdoors, conducted

---

41 See Rogalski, M., *Kontrola korespondencji*, Warszawa, 2016, pp. 101–114; the Supreme Court resolution of 21 March 2000, I KZP 60/99, *OSNKW*, 2000, No. 3–4, item 26; Kurzępa, B., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Prokuratura i Prawo*, 2000, No. 11, p. 95; Hoc, S., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Orzecznictwo Sądów Polskich*, 2000, No. 11, p. 563; Wawron, M., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Państwo i Prawo*, 2000, No. 12, p. 110; Dudka, K., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Państwo i Prawo*, 2000, No. 12, p. 106; Rogalski, M., 'Uwagi dotyczące techniki kontroli rozmów w sieci telekomunikacyjnej', *Państwo i Prawo*, 2004, No. 6, p. 77 et seq.

42 See Nita, B., 'Przedmiotowy zakres podsłuchu procesowego', *Prokuratura i Prawo*, 2005, No. 9, pp. 60–69; Rogalski, M., *Kontrola korespondencji*…, op. cit., pp. 101–102; Hofmański, P., *Kodeks postępowania karnego. Komentarz*, Vol. 1, Warszawa, 2011, pp. 1319–1320 and the literature referred to therein.

43 Piątek, S., *Prawo telekomunikacyjne. Komentarz*, Warszawa, 2019, p. 81.

44 Sakowicz, A. (ed.), *Kodeks postępowania karnego. Komentarz*, Legalis, 2023, thesis 1 to Article 241.

by one person or multiple people.[45] Meanwhile, the transmission of information other than telecommunications encompasses other forms of information transmission than those defined in Article 2(27a) TL, such as electromagnetic waves emitted by monitors and other devices.[46]

Regarding the subjective scope, 'the content of other conversations and transmissions of information' aligns with 'content data' as defined in Article 3(12) of Regulation 2023/1543. The phrase 'content of other conversations or transmissions of information' pertains to voice, image, and sound data, all of which fall under the term 'content data'. This scope also corresponds to the term 'data stored in computer systems or on carriers' used in the provisions of the CCP). Consequently, the CCP contains different terms for the same category of data, namely content data. This has undoubtedly complicated the practical application of CCP provisions that use varied terms for identical data categories and has led to numerous interpretational doubts in legal doctrine (see footnote 41). Replacing the aforementioned terms with a single term, 'content data', should resolve these issues.

CONCLUSIONS

The terms used in Article 589g § 1 CCP, Article 589l § 1 CCP, Article 589w § 4 CCP, and Article 589l § 1 CCP, such as telephone call lists, other transmissions of information, data stored in computer systems or on carriers, and content of other conversations or transmissions of information, lack legal definitions. This absence hinders their practical application. These terms are employed not only in the provisions of the Code of Criminal Procedure concerning international cooperation in criminal matters but also in other CCP provisions. Moreover, the CCP references terms and provisions from other acts, particularly the Telecommunications Law and its implementation acts.

There is a need for terminological organisation within these provisions. First, ensuring terminological coherence when applying concepts related to electronic evidence in the CCP and other acts, such as the Telecommunications Law, is essential. Second, the used terms should either be legally defined or specified in a way that minimises interpretational doubts. Regulation 2023/1543 will be instrumental in this process, as it provides a general definition of 'electronic evidence'. To organise the terms used in Chapters 62a–62d CCP, it is advisable to replace 'list of telephone calls' and 'other transmissions of information' with 'traffic data' (Article 3(11) Regulation 2023/1543). Similarly, 'data stored in a computer system or on a carrier' and 'content of other conversations or transmissions of information' should be replaced with 'content data' (Article 3(12) Regulation 2023/1543). Such terminological simplification concerning evidence obtained from electronic communication will ensure that the provisions of Chapters 62a–62d

[45] Skorupka, J. (ed.), *Kodeks postępowania karnego. Komentarz*, Legalis, 2021, thesis 3 to Article 241.

[46] Lach, A., 'Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego', *Prokuratura i Prawo*, 2003, No. 10, p. 18.

CCP concerning international cooperation align with the content of Regulation 2023/1543, thereby facilitating the practical application of these CCP chapters and the said Regulation.

BIBLIOGRAPHY

Adamski, A., *Prawo karne komputerowe*, Warszawa, 2000.

Brzeziński, P., 'Glosa do wyroku Trybunału Sprawiedliwości z dnia 21 grudnia 2016 roku w sprawach połączonych C-203/15 i C-698/15', in: Opaliński, B. and Rogalski, M. (eds), *Kontrola korespondencji. Zagadnienia wybrane,* Warszawa, 2018.

Cassey, E., 'Digital Evidence and Computer Crime: Forensic Science', *Computers and the Internet*, Baltimore, 2000.

Dudka, K., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Państwo i Prawo*, 2000, No. 12.

Dudka, K., *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin, 1998.

Dudka, K., 'Zatrzymanie korespondencji w projekcie kodeksu postępowania karnego z 1995 r. na tle przepisów obowiązujących', *Prokuratura i Prawo*, 1996, No. 4.

Ferenc-Szydełko, E., *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Legalis, 2014.

Hoc, S., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Orzecznictwo Sądów Polskich*, 2000, No. 11.

Hofmański, P., *Kodeks postępowania karnego. Komentarz*, Vol. 1, Warszawa, 2011.

Hofmański, P., 'Komentarz do wybranych przepisów Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności', in: Zielińska, E. (ed.), *Standardy Prawne Rady Europy. Teksty i komentarze. Tom III. Prawo karne*, Warszawa, 1995.

Klimczak, J., Wzorek, D., Zielińska, E., *Europejski nakaz dochodzeniowy w praktyce sądowej i prokuratorskiej – ujawnione problemy i perspektywy rozwoju*, Warszawa, 2022.

Kunicka-Michalska, B., 'Przestępstwa przeciwko ochronie informacji', in: Wąsek, A. (ed.), *Kodeks karny. Komentarz*, Vol. II, Warszawa, 2010.

Kurzępa, B., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Prokuratura i Prawo*, 2000, No. 11.

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

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

Lambert, P., 'The Search for Elusive Electrons: Getting a Sense of Electronic Evidence', *Judicial Studies Institute Journal*, 2001, No. 1.

Nita, B., 'Przedmiotowy zakres podsłuchu procesowego', *Prokuratura i Prawo*, 2005, No. 9.

Oręziak, B., 'Dowody elektroniczne a sprawiedliwość procesu karnego', *Prawo w Działaniu*, 2020, No. 41.

Piątek, S., *Prawo telekomunikacyjne. Komentarz*, Warszawa, 2019.

Rogalski, M., 'Are the Regulations with Respect to the Retention and Provision of Communications Data Appropriate in Poland? Proposals for Changes', *Ius Novum*, 2015, No. 2.

Rogalski, M., *Kontrola korespondencji*, Warszawa, 2016.

Rogalski, M., 'Uwagi dotyczące techniki kontroli rozmów w sieci telekomunikacyjnej', *Państwo i Prawo*, 2004, No. 6.

Rojszczyk, M., 'Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna', *Państwo i Prawo*, 2023, No. 2.

Szpunar, M., in: Kornobis-Romanowska, D., Łacny, J., Wróbel, A. (eds), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, Vol. III, Warszawa, 2012.
Sakowicz, A. (ed.), *Kodeks postępowania karnego. Komentarz*, Legalis, 2023.
Skorupka, J. (ed.), *Kodeks postępowania karnego. Komentarz*, Legalis, 2021.
Szumiło-Kulczycka, D., in: Skorupka, J. (ed.), *System prawa karnego procesowego. Dowody*, Vol. VIII, part 3, Warszawa, 2019.
Taras, T., 'O dopuszczalności i legalności podsłuchu telefonicznego', *Annales UMCS*, section G, Lublin, 1960.
Taylor, M., Haggerty, J., Gresty, D., Hegarty, R., 'Digital evidence in cloud computing systems', *Computer Law & Security Review*, 2010, No. 3.
Wawron, M., 'Glosa do uchwały SN z 21 marca 2000 r., I KZP 60/99', *Państwo i Prawo*, 2000, No. 12.

Cite as:

Rogalski M. (2023) *'The concept of evidence obtained from electronic correspondence'*, Ius Novum (Vol. 17) 4, 1–14. DOI 10.2478/in-2023-0026