VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

CROSS-BORDER ACQUISITION OF DIGITAL DATA IN CRIMINAL PROCEEDINGS. STATE OF PLAY AND MEASURES TAKEN BY THE EUROPEAN UNION AND THE COUNCIL OF EUROPE

Michał Gębicki, MA[1]
DOI: https://doi.org/10.7220/2029-4239.29.1

SUMMARY

The rapid development of technology has equipped us with a wide range of devices that accompany us in our daily lives. Each of these devices leaves behind a specific digital footprint, taking the form of digital data. This makes it possible to determine, for example, our location, how long we use the device or what content we download, store or transmit using our device. All of this data can then be used as evidence in criminal proceedings, which has become increasingly common in recent years. This does not only apply to crimes committed entirely via ICT networks, but also to more traditional crimes where traces are left behind in digital form. However, digital data is far different in nature from the evidence traditionally used in criminal proceedings. Prompt action by the authorities is essential to be able to obtain them and protect them from destruction or modification, even more so than for other sources of evidence. Existing methods of obtaining such data, especially cross-border acquisition, do not take into account the specific nature of digital data, as they are too time-consuming. In addition, existing cooperation frameworks are often fragmented and incomplete, which makes it all the more difficult to obtain such data efficiently. This often makes it difficult or even impossible for the authorities to achieve one of the basic objectives of criminal proceedings - identification and conviction of the perpetrator. Unfortunately, these issues are not widely discussed, despite their considerable importance for practice.

This article, due to the extensive and multifaceted nature of the subject matter discussed, cannot be treated as an exhaustive study of the issue. It is, however, a concise introduction to the problems related to the definition of digital data, methods of their cross-border acquisition and measures taken in order to improve the possibility of their acquisition by authorities conducting criminal proceedings.

[1] Author is a PhD candidate at Doctoral School at University of Silesia in Katowice, Poland.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

KEY WORDS

Digital data, cross-border acquisition of data, direct access, judicial cooperation, direct cooperation.

INTRODUCTION

It is a truism to say that the law is always one step behind the surrounding reality. This is particularly evident in the age of dynamic technological development, whose achievements often escape the existing legal framework.

This is also seen in the case of the authorities responsible for conducting criminal proceedings at the pre-trial stage. One of the problems encountered is the cross-border acquisition of digital data that could be used as evidence in criminal proceedings.

The framework for international cooperation in this area is fragmented and based on instruments that were developed at a time when the importance of digital data was not so significant. This results in the inadequacy of these tools to acquire digital data from other jurisdictions. This hinders their effective acquisition, which negatively affects the ability to conduct criminal proceedings, which are impeded at their earliest stage, namely at the stage of gathering evidence.

This inadequacy and the resulting problems have fortunately been recognised and three acts are now awaiting entry into force, which should improve the situation

The purpose of this article is, first of all, to give an overview of how the author defines the concept of digital data and how it relates to digital data and electronic (or digital) evidence. The specific features of digital data, which clearly distinguish it from other evidentiary sources that can be used in criminal proceedings, will also be presented. Next, the importance of digital data for criminal proceedings will be discussed, using the European Union as an example, as well as the channels for accessing digital data, along with an indication of their drawbacks that affect the ability to obtain them effectively. It will also be pointed out how the difficulties in effectively acquiring digital data affect the possibility of further conduct of such proceedings. Finally, the steps taken by the European Union and the Council of Europe to solve existing problems with the acquisition of digital data will be discussed, and selected specific issues related to the acts adopted by the previously mentioned entities will be compared.

DEFINITIONS

Before proceeding to the matter to which this article is mainly devoted, i.e. the importance of digital data for criminal proceedings, the ways of its cross-border acquisition and the measures adopted to improve its acquisition, it is, in the author's opinion, necessary to make some preliminary remarks which will make it possible to define precisely in which sense the author uses the notion of digital data.

This necessity is dictated by the lack of linguistic consistency which can be noticed between particular legal acts and scientific publications devoted to this issue. This inconsistency is mainly

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

due to the lack of a commonly accepted definition. As a result, one may encounter different terms, which in fact refer to one and the same category of data. These terms include inter alia digital data[2], electronic data[3], computer data[4], electronic evidence[5] (or evidence in electronic form[6]) and digital evidence[7].

Electronic, digital and analogue data

It is author's opinion that it is best, before going into more technical details, to point out the need to distinguish between electronic data and digital data.

While it constitutes a certain simplification, it can be said that electronic data means data recorded by an electronic device.

From the category of electronic data, two further categories of data can be distinguished, that is data recorded in digital form (digital data) or in analogue form (analogue data). The criterion distinguishing them is not the type of device with which they are recorded or reproduced, but the nature of the signal carrying the information[8].

Digital signal uses discrete (discontinuous) symbols generated by digital modulation, each of which can take on one of only a finite number of values, to represent information and takes a form of square wave. As such digital data takes the form of an orderly sequence of digits, zeros and ones, written using the binary number system. CDs and DVDs can serve as examples of digital data storages.

Analogue signal, on the other hand, uses continuous range of values that vary continuously with time to represent information and takes form of *sinusoidal wave. Example of medium that store analogue data are magnetic tapes, not that long ago commonly used both in video and audio cassettes.*

Considering the above, when referring to transborder acquisition of data by competent authorities it is not strictly wrong to use term electronic data. However, as described, notion of electronic data is broader than that of digital data. While there is some overlap between the concepts of electronic data and digital data, it is not justified to use those terms interchangeably.

Regarding previously mentioned computer data, it is defined in Article 1c of *Convention on Cybercrime* as "any representation of facts, information or concepts in a form suitable for

[2] P. Lewulis, Dowody cyfrowe–teoria i praktyka kryminalistyczna w polskim postępowaniu karnym (Digital Evidence – Theory and Practice in Polish Criminal Trial), (Wydawnictwo Uniwersytetu Warszawskiego, 2021), 32

[3] C. Warken, "Classification of Electronic Data for Criminal Law Purposes", The European Criminal Law Associations' Forum, Issue 4/2018, 226 // DOI: 10.30709/eucrim-2018-023 //

[4] Convention on Cybercrime (ETS No. 185), Article 1c; Polish Code of Criminal Procedure (Act of 6 June 1997-Code of Criminal Procedure), Journal of Laws of the Republic of Poland, 2024, no. 37, inter alia Article 143 § 1.6, Article 218a § 1-2, Article 218b.

[5] P. Oręziak, "Dowody elektroniczne a sprawiedliwość procesu karnego" ("Electronic Evidence and the Fairness of the Criminal Trial"), Prawo w Działaniu, 41/2020, 190 // DOI: 10.32041/pwd.4110 //

[6] Convention on Cybercrime (ETS No. 185), inter alia Preamble, Article 14.2c, Article 23.

[7] Europol. "SIRIUS EU Digital Evidence Situation Report 2019", 20 December 2019, https://www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-2019 [last access on: 11 May 2024]

[8] P. Lewulis, Dowody cyfrowe…, 32

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

processing in a computer system, including a program suitable to cause a computer system to perform a function"[9]. On the other hand, while *Polish Code of Criminal Procedure* invokes this term in several articles, it does not provide any insight as to how this term should be understood. Nevertheless, while computer data is defined in a legally binding way, author shares the view that said definition, when considered from the perspective of technical sciences, is not satisfactory since it is not substantially clear[10], therefor author will abstain from utilising this term.

As such, for the purpose of this paper digital data should be understood as data recorded by electronic device using discrete values within binary number system.

Electronic and digital evidence

When discussing electronic and digital evidence, two issues should be taken into account.

First, above mentioned differences between scope of meaning of terms electronic and digital remain fully valid and are applicable.

Second, author supports position that at the stage of collection of data using term evidence is not appropriate. Using term evidence presupposes that gathered data is admissible in criminal proceeding and that it will have probative value[11]. Therefore notions of electronic or digital evidence should only be used when data is admissible as evidence and holds probative value.

Since term evidence holds neutral meaning, it is more appropriate to use it at the stage of collection of data by competent authorities and as such it will be used by author.

CHARACTERISTICS OF DIGITAL DATA

In view of the previous definition of digital data, it is necessary to proceed to the indication of the features which distinguish it from other evidence which may be used in criminal proceedings. Indeed, these specific features have far-reaching consequences for practice, both in terms of their acquisition and subsequent use as evidence in criminal proceedings.

Immateriality and abstractness

As indicated earlier, electronic evidence is merely an ordered sequence of digits written in binary system. This determines their first specific characteristics, namely immateriality and abstractness. This statement is not contradicted by the fact that data is stored on tangible media,

[9] Convention on Cybercrime, supra note 4, Article 1c

[10] P. Lewulis, Dowody cyfrowe…, 32

[11] S. V. Maymir, "Anchoring the need to revise cross-border access to e-evidence", Internet Policy Review, Vol. 9, issue 3, September 2020, 4 // DOI: 10.14763/2020.3.1495 //; European Parliament. Committe on Civil Liberties, Justice and Home Affairs, *Draft report on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters* (Draft Report 2018/0108(COD)), 24 October 2019, 147-148

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

such as memory sticks or hard disks.. Evidence in proceedings will always be the content of a digital record itself and not the medium on which it is stored[12].

Ease of storage

Digital data is easily stored. Thanks to rapid advances in technology, existing data storage media today offer very high storage capacity while remaining small in size. From the user's point of view, this is an unquestionable advantage, but for the investigating authorities it often results in the necessity to painstakingly search the media for one particular sequence of data or to search for easily concealed data carriers as part of their operations[13].

Ease of replication

Due to its nature, digital data is easily copied. In practice, this means that the transfer of digital data that constitutes evidence in a proceeding, unlike evidence in the traditional sense, does not necessarily mean that the original data holder loses control over the data. Typically, the data holder retains the original dataset and transfers only a copy of it, and that copy can be transferred electronically, on a portable data storage device or even in the form of a paper printout[14].

It should be emphasized that the evidentiary value of digital data in proceedings depends on its integrity. It is therefore crucial to be able to prove that the content presented as evidence in the proceedings is exactly the same as its original, hence a strong emphasis should be placed on the use of appropriate methods of authenticating copies of transmitted data[15].

Susceptibility to modification and loss

Even everyday life experience suggests that digital data is susceptible to modification and loss. Interference with the integrity of digital data can occur either intentionally or accidentally.

As an example of intentional interference with digital data, one can point to hiding the place of origin of the data, the entity from which the data originated, for example, through the use of VPN (Virtual Private Network) systems or anonymous networks, such as Tor, which use second-generation onion routing. It is also possible to hide or modify the original data, using communicators encryption or messengers that use scripts that allow the transmitted data to self-

[12] P. Karasek, "Gdy dowodem są dane – czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych" ("Digital data as evidence – truths and myths about digital evidence acquisition"), Edukcja Prawnicza No. 2/2015, 22

[13] P. Lewulis, Dowody cyfrowe…, 32

[14] C. Warken, supra note 3, 227

[15] P. Lewulis, "Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law", Criminal Law Forum, Vol. 33 (2022), December 2021, 44 // DOI: 10.1007/s10609-021-09430-4 //

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

destruct. All of these activities are aimed at obliterating traces and prevent digital data from being used as evidence in criminal proceedings. criminal proceedings.

Unintentional interference with data integrity, on the other hand, can occur even in the course of ordinary device use. Digital data can be overwritten on the same media, resulting in the loss of the original version, or the data may not be saved at all, whether through system user error or a sudden power supply cut. Similarly, it is easy to change attributes of a file containing digital data, such as the time of last access. This is because they are subject to change every time such a file is opened such a file[16].

THE RELEVANCE OF DIGITAL DATA FOR CRIMINAL PROCEEDINGS

Due to the rapid development of technology over the last decades, digital data are becoming increasingly valuable as evidence in criminal proceedings.

Sometimes, due to the specific nature of certain criminal acts offences, such as those committed in cyberspace, they can often constitute the only means of evidence that will allow responsibility to be allocated to the perpetrators[17]. This is particularly important in view of the increasing professionalisation of those involved in cybercrime activities.

Furthermore, over the past few years it has been observed that digital data is not only relevant in the context of classic cybercrimes such as DDoS attacks or ransomware attacks, but also in the context of traditional crimes such as fraud or sexual exploitation of minors, which are increasingly being committed via the Internet[18].

Unfortunately, however, it is difficult to provide a detailed picture of the scale of the use of digital data in criminal proceedings. This is due to the pragmatics of the authorities' record-keeping and statistics. While it is more likely that the use of digital data as evidence is recorded in the files kept, information on what type of evidence was used in a given proceeding is not included in published statistics on, for example, the number of crimes detected or the number of convictions.

Rudimentary, but research-based, approximation of the scale of the phenomenon can be done thanks to is to refer to the results of an open consultation conducted by the European Commission[19]. Said survey was aimed at gathering feedback on the practice so far developed by European Union Member States regarding the acquisition of electronic evidence. The purpose of the collected data was to find out the current legal framework regulating the use of electronic evidence in the Member States and the admissibility of its use in criminal proceedings, as well as

[16] P. Lewulis, Dowody cyfrowe…, 65
[17] P. Oręziak, supra note 5, 189
[18] C. Warken, supra note 3, 226
[19] European Commission. Commission Staff Working Document-Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, 17 April 2018

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

practical problems with obtaining such evidence, both at the national and international level, resulting from gaps in the regulation of this matter. The aim was also to assess whether there was any need to attempt to regulate this issue at EU level.

Bearing in mind previous remarks in regards to meaning of terms digital data and electronic evidence, notion electronic evidence was used for the purpose of conducting the survey. As such, it will also be used by the author within this subsection of the paper.

As per the wording of Impact Assessment *"the survey comprised four main parts combining cooperation channel and location of the counterpart criterions. The requested data were broken down into eight respective categories based on its nature and type of the service provider, i.e. electronic communication services, telecommunication services, and internet or app-based service"*[20].

Based on the gathered data it was determined that electronic evidence in any form is relevant to approximately 85% of all criminal proceedings at pre-trial stage. Furthermore, in roughly 65% of those cases there is a need to acquire electronic evidence from another jurisdiction. As such, combining both numbers suggests that electronic evidence is relevant in almost 55% of all criminal investigations[21].

These data illustrate that the importance of digital data for the effective conduct of criminal proceedings is enormous. The problem discussed in the framework of this article is not only theoretical, but is embedded in the current problems faced by the authorities.

At the same time it should be noted that said numbers are not precise, which is admitted by European Commission itself[22]. Method of carrying out the research has also been criticised[23]. Unfortunately, while it undermines the reliability of said statistics, to the author's best knowledge, it remains a sole source of somewhat reliable information regarding this topic. It should be kept in mind, when data gathered for the purpose of Impact Assessment is invoked in the following part of this paper.

CHANNELS OF TRANSBORDER ACCESS TO DIGITAL DATA IN CRIMINAL PROCEEDINGS AND THEIR SHORTCOMINGS

In criminal cases where there is a need for transborder acquisition of data authorities may make us of one (or more than one) methods (channels) of access, that is:

1. Direct access
2. Judicial cooperation
3. Direct cooperation

[20] Ibid., 258
[21] Ibid., 14
[22] Ibid., 13
[23] For further insight- S. V. Maymir, supra note 11

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

Direct access

Direct access refers to cases where authorities access data stored abroad themselves. This means that there are no intermediaries, such as authorities of another state or private entities.

The essence of this method is, broadly speaking, to examine system within which data is stored from another system. It can take form of either extended search or remote search[24].

Extended search refers to instances in which following the seizure and examination of a device (primary system) it is revealed that data that may hold probative value is stored in another system (secondary system) that can be accessed via the primary system. In such cases search is extended to secondary system[25]. The possibility of conducting of extended search is in principle case-dependent and incidental and cannot be treated as a certain source of data acquisition. A the same time, it is possible for authorities to seize and search primary system purely based on knowledge that secondary system can be searched this way. However it can be said with a high degree of certainty that these are extremely rare cases.

In case of remote search examination follows prior acquisition of login information, that allows access to system in which data is stored. As such, contrary to extended search targeted system is predetermined by authorities. Login information can be obtained in multitude of ways, including use of remote forensic software, such as Trojans or key-loggers[26], produced during an interrogation or obtained during a search, if someone is careless enough to save access data to their accounts.

While direct access allows for relatively quick access to data it still is subject to a number of drawbacks, particularly in the context of cross-border access.

First limitation is the admissibility of this method under the laws of the country whose authorities are carrying out the search. Although the legal orders of at least 20 of the European Union Member States allow authorities to carry out extended searches, only in a few of those States it is permissible to carry out remote searches[27].

Another, in the author's opinion more serious, limitation to the effective use of of these methods of access to digital data lies in jurisdictional issues. Even if national law allows for the use of remote or extended search, it should be considered that the possibility of conducting such search is limited to systems located within the territory in which the authorities may exercise their jurisdiction. Violation of the territoriality principle constitutes interference with one of the basic components of state sovereignty. Thus, it should be deemed unacceptable to conduct remote or extended search of systems located in another country's jurisdiction without first obtaining the consent of its competent authorities, which obstructs possibility of timely acquisition of data[28].

[24] European Commission, supra note 19, 11

[25] A. Lach, "Przeszukanie na odległość systemu informatycznego" ("Remote search of an IT system"), Prokuratura i Prawo, 9/2011, 68

[26] Ibid.

[27] European Commission, supra note 19, 11

[28] A. Choroszewska, P. Opitek, "Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany, cz. II" ("Obtaining digital evidence abroad: existing legislation and amendments under way (Part II)"), Prokuratura i Prawo, 2020, 10-11/2020, 215

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

Major questions should also be raised with regard to the proportionality of interference with the right to privacy of a user of an information system. However, these issues require a detailed discussion that would go beyond the scope of this paper.

Judicial cooperation

Judicial cooperation between authorities of states, within the framework of mutual legal assistance systems, is a channel of access that eliminates the jurisdictional problems described earlier. Judicial cooperation systems are designed to ensure respect for the sovereignty of states on whose territory certain types of action are to be carried out.

While utilising this route authorities of one country make a formal request to the competent authorities of the country on whose territory digital data is located. If the request is granted, the data specified therein is obtained using the means provided for in the legal order of the State whose authorities are the addressee of the request and transmitted to the authorities of the requesting State[29].

Judicial cooperation is carried primarily by system of mutual legal assistance treaties. Said treaties can be either bilateral, such as *Treaty between the Republic of Poland and the Republic of Lithuania on Legal Assistance and Legal Relations in Civil, Family, Labour and Criminal Matters of 26 January 1993*[30] or multilateral, such as previously invoked *Convention on Cybercrime*[31]. Between Member States of the European Union judicial cooperation can also be carried within framework of *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.*

The criticisms directed at both of those cooperation schemes focus mainly on the delays associated with the obligation to subject data requests to judicial validation, in most cases both in the state which authorities request data and in the state from which data is to be obtained in. The involvement of the competent judicial authorities is intended to prevent possible jurisdictional disputes and is also intended to mutually verify that data access requests comply with applicable rules, both national and international[32].

When it comes to European Investigation Order time limit for recognition of an order is 30 days unless grounds for postponement occur[33] and time for execution of order after its recognition

[29] European Commission, supra note 19, 11

[30] Treaty between the Republic of Poland and the Republic of Lithuania on Legal Assistance and Legal Relations in Civil, Family, Labour and Criminal Matters of 26 January 1993, Journal of Laws of the Republic of Poland, 1993, no. 130

[31] Convention on Cybercrime, supra note 4

[32] M.Stefan, G. G. Fuster, "Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US", CEPS Papers in Liberty and Security in Europe, No. 2018-07 (November 2018), 2

[33] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Official Journal of the European Union, L 130/1, Article 12.3-12.4

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

can vary between 90 and 120 days[34]. Despite provided time limit in practise delays exceeding 6 months or even a year occur[35].

Time needed to acquire data within framework of mutual legal assistance treaties can be even lengthier. In previous instances of cooperation between members States of the European Union with non-member states in roughly 20 % of cases data is transferred within 1 month. Instances when response comes within 1 to 6 months amount to roughly 40% of all cases, within 6 to 12 months 28% and after a year-12%[36].

Given the specific nature of digital data, its susceptibility to loss and modification, time necessary to obtain digital data via the European Investigation Order or mutual legal assistance makes it difficult, and in some cases impossible, to obtain it efficiently. Hence, it is argued that these models of formal cooperation are outdated (despite the fact that the *Directive 2014/41/EU* came into force in May 2017, so the instrument itself has been in use for a relatively short period of time), as being unsuited to the acquisition of digital data, leading to their relatively low efficiency[37].

Another obstacle that can in some cases prevent effective use of the European Investigation Order or mutual legal assistance is the phenomenon of so-called loss of knowledge of location[38].

This situation occurs when it is not possible to determine the location of digital data storage at all, or the place of storage is constantly changing. In the case of a complete loss of knowledge of location, the use of these instruments will not be possible at all, as they require a request for data to the competent authorities of a specific country. If the location of the data changes, it will be possible to apply to another country to secure and release the data, but there is a risk that their location will change in the process. If, as a result of the change of location, the data will be in a jurisdiction other than the original one, it will be necessary to make a new request to the competent authorities of yet another state.

Direct cooperation

Third channel of access to digital data that authorities may use is direct cooperation with the private entity holding the data, most often the service provider.

As the name suggests, under the direct cooperation model, the competent authorities contact service providers directly and request them to release data, without the involvement of the authorities of the State whose law binds the service provider.

The actual scale of the use of this method of cooperation has been and continues to be difficult to assess, due to the scarcity of data. However, on the basis of surveys carried out among

[34] Ibid., Article 12.5-12.6

[35] European Commission, supra note 19, 263

[36] Ibid.

[37] P. Swire, J. Hemmings, S. Vergnolle, "A Mutual Legal Assistance Case Study: The United States and France", Wisconsin International Law Journal, 323 (2017), 324 // DOI: 10.2139/ssrn.2921289 //

[38] Sometimes also simply called loss of location. However, term loss of knowledge of location seems more appropriate, since it refers to loss of location not in the ontological sense but in the epistemological sense. See- B. J. Koops, M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law", Tilburg Law School Research Paper, No. 5/2016, 3-4 // DOI: 10.2139/ssrn.2698263 //

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

the Member States of the European Union, it is possible to make a rough estimate of the scale of use of this method.

In 2013, nearly 71 500 requests for data were made directly to service providers by the authorities of the Member States of the European Union. The number of cases in which data were issued (either in full or only partially) was in the range of 45%. In 2014, the number of requests was just over 79 000 with around 44 % of them were fulfilled. 2015 saw a dynamic increase in the number of requests, exceeding 100 00, with around 46% of requests realised, achieving a success rate similar to previous years. 2016 again saw a significant increase in the number of applications, reaching over 120 000. Success rate also significantly increased, to approximately 55%[39].

Analysis of collected data shows an increase in the number of requests made from around 71,500 in 2013, to more than 120,000 in 2016, an increase of roughly 70% over four years. In this time frame have requested the release of data nearly 9,000 times. In 2013, the number was almost 1 600 and in 2016 it exceeded 3 200, more than doubling. In the same period, Lithuanian authorities made slightly more than 400 requests, of which 36 in 2013 and almost 160 in 2016, which translates into an increase of almost 4.5 times[40].

Data for the time frame after 2016 is not available, however, with certain degree of safety it can be assumed that following years also saw increase in number of requests. Nonetheless, this shows a significant increase in the importance of working directly with service providers as a channel for obtaining digital data for criminal proceedings.

Practice also shows that time it takes service provider to direct request for release of data is substantially shorter than in case of European Investigation Order or mutual legal assistance

Waiting time for a response to a direct data request to EU service providers does not exceed 10 days in about 50% of cases. About 20% of responses are received by the authorities within 11 to 30 days and about 29% between 1 and 6 months. Cases where the response time exceeds one year represent less than 1% of all cases.

With regard to cooperation with non-EU service providers, the statistics look slightly worse, but still significantly better than in the case of judicial cooperation. In roughly 33 % of cases answer arrives within 10 days, in approximately 30% instances within 11 to 30 days and within 1 to 6 months in 27% of cases. Surprisingly, within years 2013-2016 there was no instance when it took non-EU service provider more than 12 months to respond.

Unfortunately, despite the above rather favourable statistics, this method of accessing data also suffers from drawbacks that make it difficult to use in practice.

First of all, it is possible only insofar as the relevant regulations of particular States allow this form of cooperation at all.

Still, even if the relevant national legislation allows authorities to request release of data and service providers to release said data, the effective use of this access channel is hindered by the lack of regulation of the rules of such cooperation. The willingness of service providers to cooperate with the competent authorities must therefore be entirely voluntary, as there are no instruments forcing the release of data. Therefore, in practice, the release of data depends on the service provider's internal regulations, in which they set their own requirements for requests,

[39] European Commission, supra note 19, 267
[40] Ibid., 268

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

taking into account the law applicable to them, but also the specifics of their services and products. This reflects negatively on the percentage of fulfilled requests[41].

It should also be noted that this channel of access does not provide sufficient guarantees towards the rights of data subjects. Author supports the position that the assessment of the legality and proportionality of the requests should remain the domain of competent state authorities, while the current design of this avenue of cooperation places service providers, as it were, in the role of both law enforcers and adjudicators[42].

THE IMPACT OF DIFFICULTIES IN CROSS-BORDER ACQUISITION OF DIGITAL ON CRIMINAL PROCEEDINGS

The difficulties in using existing methods of obtaining digital evidence data, as typified above, unfortunately negatively affect the ability to effectively carry out criminal proceedings.

Table 1 presents figures for pre-trial proceedings negatively affected by difficulties in obtaining electronic evidence[43].

TABLE 1

Percentage of criminal proceedings (at pre-trial stage) negatively affected by difficulties in obtaining digital data44

Cause	Within the EU With non-EU countries		With non-EU countries	
	Judicial cooperation	Direct cooperation	Judicial cooperation	Direct cooperation
Lack of timely access	35 %	25 %	45 %	15 %
Lack of access (access denied)	25 %	25 %	25 %	15 %
Other	15 %	5 %	15 %	10 %
Total	**75 %**	**55 %**	**85 %**	**40 %**

[41] See Table 1 below

[42] S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors", Computer Law & Security Review, 2021, Vol 43, 9 // DOI: 10.1016/j.clsr.2021.105614 //

[43] Table 1 contains data only on incidents of authorities' use of from the channels of judicial cooperation and direct cooperation. This should not come as a surprise, since even if the authorities of particular states use methods of direct access to data, it should be assumed that this information would not be disclosed as part of the EU consultations.

[44] European Commission, supra note 19, 259

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

As can be seen, the difficulty with effective cross-border acquisition of digital data negatively impacts between 40% to 85% of all pre-trial proceedings. Consequently, the further prosecution was far more difficult, or even impossible at all. Data also allow to conclude that in the vast majority of cases, the use by the authorities of the channel of direct cooperation with the service provider in possession of digital data, despite the partial, or lack thereof, regulation of this channel of access, is characterized by a significantly higher efficiency than the use of channels of cooperation between the authorities of the countries within the framework of European Investigation Order or mutual legal assistance.

MEASURES TAKEN BY THE EUROPEAN UNION AND THE COUNCIL OF EUROPE

The previously highlighted difficulties with the effective cross-border acquisition of digital data in criminal proceedings have fortunately not gone unnoticed. Efforts to adopt acts to improve the situation have been undertaken by a number of different actors, however, due to the subject scope of this article, the following will focus on the actions taken by the European Union and the Council of Europe.

Background

In both cases, steps to improve digital data acquisition capabilities were taken at approximately the same time.

At EU level, the need for improvement was already signalled in The European Agenda on Security of 28 April 2015[45]. This necessity was also signalled several times thereafter. Work on the draft act was significantly accelerated due to the terrorist attacks that were committed in Brussels on the morning of 22 March 2016. A series of coordinated terrorist attacks, carried out by suicide bombers, took place on that day. Two of the charges were detonated at Brussels Airport, while the third was detonated at the Brussels Maelbeek/Maalbeek metro station. The attacks resulted in the deaths of 32 people and wounded more than 300.

In the Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU, issued two days after the attacks, it was deemed a priority "to find ways […] to secure and obtain more quickly and effectively digital evidence"[46].

The efforts made have led to the publication on 17 April 2018 drafts of two acts, namely *Proposal for a Regulation of The European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*[47] (hereinafter:

[45] European Commission. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. The European Agenda on Security, 28 April 2015

[46] https://www.consilium.europa.eu/en/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

Proposal for Regulation) and *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[48] (hereinafter: Proposal for Directive). Both of them are referred to as *E-Evidence package.*

The legislative process was long and arduous. Initially, the drafts were widely debated and then went into the so-called legislative freezer. Once work on them was resumed, a difficult trilogue between the relevant institutions of the European Union ensued and for a long period it seemed that agreement on the final form of the regulation would not be reached. Ultimately, consensus was reached.

In regards to the Council of Europe it has been noted in the T-CY assessment report of 3 December 2014 that parties to *Convention on Cybercrime* should enhance direct cooperation between judicial and also "may consider addressing the practice of law enforcement and prosecution services obtaining information directly from foreign service providers, and related safeguards and conditions"[49].

Between September 2017 and May 2021 over ninety sessions of the T-CY Protocol Drafting Plenary, Drafting Group and Sub-groups as well as six rounds of stakeholder consultations were held[50].

Ultimately *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* was approved by the Committee of Ministers on 17 November 2021[51].

Adopted acts

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224; hereinafter: Second Additional Protocol) was opened for signature by the States Parties to Convention on Cybercrime (ETS No. 185) on 12 May 2022[52].

A little more than a year later, on 12 July 2023 *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*[53] (hereinafter: Regulation (EU) 2023/1543) and *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*

[48] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN

[49] Cybercrime Convention Committee. T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014, 127

[50] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group [last access on: 10 May 2024]

[51] Ibid.

[52] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)

[53] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Official Journal of the European Union, L 191/118

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings[54] (hereinafter: Directive (EU) 2023/1544) were adopted and consequently published in the Official Journal of the European Union on 28 July 2023.

Both acts pave the way for legislation regulating the conditions for competent authorities to cooperate with entities holding digital data under the direct cooperation route. This represents a global breakthrough and milestone.

Approach to direct cooperation and judicial cooperation

Regulation (EU) 2023/1543 introduces two new instruments, aimed at making acquiring digital data easier. First is European Production Order (hereinafter: EPOC), obliging service providers to release data requested by competent authorities[55]. Second is European Preservation Order (hereinafter: EPOC-PR), which serves as a way of, as a name implies, preservation of data for the purposes of a subsequent request for release of data under EPOC[56]. Both instruments shall be applicable within scheme of direct cooperation with service providers.

At the same time *Regulation (EU) 2023/1543* provides procedure for enforcement in case of non-compliance with EPOC or EPOC-PR by service provider. In such cases authority issuing EPOC or EPOC-PR may request the competent authority of another Member State to enforce release of data. As such, when obtaining data under direct cooperation is not possible the judicial cooperation is set into motion.

The way in which data acquisition is regulated in *Second Additional Protocol* should be regarded as particularly interesting. Contrary to *Regulation (EU) 2023/1543* whether data will be obtained by direct cooperation or judicial cooperation is determined by type of data.

In regards to domain name registration information and subscriber information direct cooperation is prescribed and when it comes to subscriber information and traffic data judicial cooperation is employed[57].

It is expressed directly that possibility to obtain subscriber data by judicial cooperation is envisioned particularly for the instances of non-cooperation by service provider previously requested to release data under direct cooperation[58]. However, it should be considered that not providing for such a possibility in relation to a domain registration name is incomprehensible. In the light of the above, it should be assumed that in cases where service providers do not release domain registration name under direct cooperation authorities issuing the request will not be able to invoke provisions of *Second Additional Protocol* and will have to employ judicial cooperation within framework of other acts relating to mutual legal assistance.

[54] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, Official Journal of the European Union, L 191/118

[55] Regulation (EU) 2023/1543, supra note 51, Art. 3.1

[56] Ibid., Art. 3.2

[57] Ibid., Art. 6-8

[58] Second Additional Protocol, supra note 50, Art. 7.7

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

Time to release data

As mentioned previously one of the drawbacks of existing framework of cooperation untimely release of data is one of the most crucial drawbacks. Both the *Regulation (EU) 2023/1543 and Second Additional Protocol* aim to tackle this issue.

Regulation (EU) 2023/1543 provides that requested data, as a general rule, should be released within 10 days of reception of EPOC. In emergency cases however, the addressee shall transmit the requested data without undue delay, at the latest within eight hours following receipt of the EPOC[59].

Such a significant reduction in time to release data is a huge improvement on the current situation. At the same time, however, it raises concerns about the service provider's ability to reliably verify during this time that the conditions for data release have been met. There is no doubt that it is desirable to speed up the acquisition of data by authorities conducting criminal proceedings. However, this must not lead to a violation of the principle of proportionality of interference with the privacy of data subjects

When it comes to EPOC-PR data should be preserved without undue delay. Data should be preserved for 60 days, unless the EPOC has been issued-in such cases obligation to preserve data does not cease. Additionally, within those 60 days the authority issuing EPOC can extend the duration of the obligation to preserve the data for additional 30 days[60].

Second Additional Protocol does not introduce as uniform regulations in relation to the time within which service providers are to release data.

In regards to request for domain name registration information and disclosure of subscriber information the time frame within data should be transmitted by service provider to requesting authority is to be decided by the authority itself[61]. However, such an approach raises concerns similar to those raised in relation to the time of release of data under EPOC. There is a risk that authorities will impose very short deadlines on service providers for the release of data, making it difficult or even impossible for them to reliably assess the justification for the release of data.

When it comes to judicial cooperation on obtaining subscriber information and traffic data time limits are laid down both for the authority to transmit the request for data and for the service provider to release the data.

Competent authority should serve the request to the service provider within 45 days of its receipt. Time within which the service provider shall release data is 25 days subscriber information and for and 45 days for traffic data[62].

[59] Ibid., Art. 10.2-3
[60] Regulation (EU) 2023/1543, supra note 51, Art. 11.1
[61] Second Additional Protocol, supra note 50, Art. 6.3d; Art. 7.4c
[62] Second Additional Protocol, supra note 50, Art.8.6a

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

Entry into force and application

Regulation (EU) 2023/1543 entered in force on the 17th of August 2023, that is on the twentieth day following that of its publication in the Official Journal of the European Union**.** It shall apply from 18 August 2026[63].

Second Additional Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five Parties to the Convention on Cybercrime have expressed their consent to be bound by this Protocol[64].

As of 10 May 2024, the Second Additional Protocol has been signed by 41 states, of which 29 are member states of the Council of Europe and 12 are Non-Members of Council of Europe. Of the signatories, only two states have ratified the protocol-Serbia and Japan[65]. As such, at this point in time it is not possible to tell when it will enter into force.

CONCLUSIONS

1. In light of the difficulties faced by authorities in the course of cross-border acquisition of digital data in criminal proceedings, it is to be highly commended that international law actors have taken steps to improve the situation.
2. Efforts to regulate the sphere of cooperation between authorities and service providers under the direct cooperation route are undoubtedly to be commended.
3. Firstly, this will make it possible to standardise practice in this area. Secondly, it will strengthen the position of the authorities requesting data. They will no longer be in a merely servile position, able only to politely request the necessary data to be released. Instead, they will be able to issue a legally binding order to release certain categories of data. This should eliminate, or at least reduce, the number of cases in which the acquisition of digital data necessary for criminal proceedings will depend on the internal regulations of the private parties holding the data. After all, the ability of private parties to obstruct the course of criminal proceedings cannot in any way be regarded as desirable. It would not allow the fundamental objectives of criminal proceedings, that is to say the conviction of the offender, to be achieved.
4. Similarly, the provision of deadlines within which the data should be released - either by specifying the date by which the data should be released explicitly in the legislation or by leaving the setting of the release deadline to the authority requesting the data - is to be welcomed. At the same time, however, one has to ask whether setting such deadlines for data release could have a real impact on the speed of data acquisition.
5. As indicated earlier (see Direct cooperation section), the time to release data by service providers from the European Union in approximately 50% of cases does not exceed 10 days, while for service providers from outside the European Union in 33% of cases answer arrives within 10 days, in approximately 30% of instances within 11 to 30 days and within 1 to 6 months in 27% of cases. Comparing the above figures to the release

[63] Regulation (EU) 2023/1543, supra note 51, Art. 34.1-2
[64] Second Additional Protocol, supra note 50, Art. 16.3
[65] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

times set out in Regulation 1543/2023 (EU), i.e., as a general rule 10 days and 8 hours in exceptional situations, the effect of reducing release times should occur. The improvement should be observed for about 50% of cases involving service providers from the European Union and about 70% of cases involving service providers from outside the European Union.

6. Due to the different manner of the regulation with regard to the Second Additional Protocol and the fact that it is left to the competent authority to determine the time limit for the service provider to release the data, it is difficult to assess at this point whether the adopted regulation will have the desired effect. However, it should be expected that the authorities will set a relatively short deadline for the release of data.
7. At the same time, it should be noted that the regulation of the Second Additional Protocol with regard to the time for the release of data within the framework of judicial cooperation (either standalone or following a refusal by the service provider to release data within the framework of direct cooperation) should lead to an improvement of the situation. The time limit is a maximum of 70 days in relation to subscriber information and 90 days in relation to traffic data. Given that the release of data through judicial cooperation takes between 1 and 6 months in about 80% of cases (see Judicial cooperation section), it can be assumed that the application of the Second Additional Protocol will bring a noticeable improvement.
8. Of course, as signalled at the outset, the issues discussed are complex and multifaceted and cannot be considered to be exhausted by this article. A separate analysis is required, for example, of the criteria which must be fulfilled in order to request data, which authorities may request data from service providers, and whether the grounds for refusal to release data provide sufficient safeguards for the rights of data subjects. While improvements in the efficiency of data acquisition are necessary, such improvements must not come at the expense of the protection of human rights and fundamental rights and freedoms.
9. Apart from the above, the question must be raised whether the adopted acts will improve the situation. Only after the legislation has been implemented and the first practical experience in its use has been gained, will a reliable assessment be possible. Due to the distant date of entry into force, there is also a concern that the dynamic development of technology will make the adopted acts obsolete and inadequate to their stated aims from the moment of their initial application.
10. However, this concern should not come as too much of a surprise-in the end, the law is always one step behind the surrounding reality.

LEGAL REFERENCES

Literature

1. Choroszewska, A., Opitek, P. "Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany, cz. II" (Obtaining digital

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

evidence abroad: existing legislation and amendments under way (Part II)"), Prokuratura i Prawo, 2020, 10-11/2020, 195-228
2. Karasek, P., "Gdy dowodem są dane – czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych" ("Digital data as evidence – truths and myths about digital evidence acquisition"), Edukcja Prawnicza, No. 2/2015, 22-26
3. Koops, B. J., Goodwin, M., "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law", Tilburg Law School Research Paper, No. 5/2016, // DOI: 10.2139/ssrn.2698263 //
4. Lach, A., "Przeszukanie na odległość systemu informatycznego" ("Remote search of an IT system"), Prokuratura i Prawo, 9/2011, 67-80
5. Lewulis, P., "Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law", Criminal Law Forum, Vol. 33 (2022), December 2021, 39–62 // DOI: 10.1007/s10609-021-09430-4 //
6. Lewulis, P., Dowody cyfrowe–teoria i praktyka kryminalistyczna w polskim postępowaniu karnym (Digital Evidence – Theory and Practice in Polish Criminal Trial), (Wydawnictwa Uniwersytetu Warszawskiego, 2021)
7. Maymir, S. V., "Anchoring the need to revise cross-border access to e-evidence", Internet Policy Review, Vol. 9, issue 3, September 2020, 1-24 // DOI: 10.14763/2020.3.1495 //
8. Oręziak, P., "Dowody elektroniczne a sprawiedliwość procesu karnego" ("Electronic Evidence and the Fairness of the Criminal Trial"), Prawo w Działaniu, 41/2020, 187-196 // DOI: 10.32041/pwd.4110 //
9. Stefan, M., Fuster, G.G., "Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US", CEPS Papers in Liberty and Security in Europe, No. 2018-07 (November 2018),
10. Swire, P., Hemmings, J., Vergnolle, S., "A Mutual Legal Assistance Case Study: The United States and France", Wisconsin International Law Journal, 323 (2017), // DOI: 10.2139/ssrn.2921289 //
11. Tosza, S.,"Internet service providers as law enforcers and adjudicators. A public role of private actors", Computer Law & Security Review, 2021, Vol 43, 9 // DOI: 10.1016/j.clsr.2021.105614 //
12. Warken, C., "Classification of Electronic Data for Criminal Law Purposes", The European Criminal Law Associations' Forum, Issue 4/2018, 226-234 // DOI: 10.30709/eucrim-2018-023 //

Legislation

13. Convention on Cybercrime (ETS No. 185)
14. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, Official Journal of the European Union, L 191/118

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

15. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Official Journal of the European Union, L 130/1
16. Polish Code of Criminal Procedure (Act of 6 June 1997-Code of Criminal Procedure), Journal of Laws of the Republic of Poland, 2024, no. 37
17. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Official Journal of the European Union, L 191/118
18. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)
19. Treaty between the Republic of Poland and the Republic of Lithuania on Legal Assistance and Legal Relations in Civil, Family, Labour and Criminal Matters of 26 January 1993, Journal of Laws of the Republic of Poland, 1993, no. 130

Other reference

20. Cybercrime Convention Committee. T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014
21. European Commission. Commission Staff Working Document-Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 118 final, 17 April 2018
22. European Commission. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. The European Agenda on Security, 28 April 2015
23. European Parliament. Committe on Civil Liberties, Justice and Home Affairs, *Draft report on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters* (Draft Report 2018/0108(COD)), 24 October 2019
24. Europol. "SIRIUS EU Digital Evidence Situation Report 2019", 20 December 2019, https://www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-2019
25. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN
26. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN
27. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224
28. https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

29. https://www.consilium.europa.eu/en/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/

SANTRAUKA

TARPVALSTYBINIS SKAITMENINIŲ DUOMENŲ GAVIMAS BAUDŽIAMAJAME PROCESE. DABARTINĖ PADĖTIS IR PRIEMONĖS, KURIŲ ĖMĖSI EUROPOS SĄJUNGA IR EUROPOS TARYBA

Sparčiai tobulėjant technologijoms, turime daugybę prietaisų, kurie lydi mus kasdieniame gyvenime. Kiekvienas iš šių prietaisų palieka tam tikrą skaitmeninį pėdsaką - skaitmeninius duomenis. Tai leidžia nustatyti, pavyzdžiui, mūsų buvimo vietą, kiek laiko naudojamės įrenginiu arba kokį turinį atsisiunčiame, saugome ar perduodame naudodamiesi įrenginiu. Visi šie duomenys vėliau gali būti naudojami kaip įrodymai baudžiamosiose bylose, o tai pastaraisiais metais tampa vis dažniau pasitaikančiu reiškiniu. Tai pasakytina ne tik apie nusikaltimus, įvykdytus tik IRT tinklais, bet ir apie labiau tradicinius nusikaltimus, kai pėdsakai paliekami skaitmenine forma. Tačiau skaitmeniniai duomenys savo pobūdžiu gerokai skiriasi nuo tradiciškai baudžiamosiose bylose naudojamų įrodymų. Siekiant juos gauti ir apsaugoti nuo sunaikinimo ar pakeitimo, būtina, kad valdžios institucijos galėtų imtis skubių veiksmų dar labiau nei kitų įrodymų šaltinių atveju. Taikant esamus tokių duomenų gavimo būdus, ypač kalbant apie tarpvalstybinį duomenų gavimą, neatsižvelgiama į specifinį skaitmeninių duomenų pobūdį, kadangi tai užima pernelyg daug laiko. Be to, esamos bendradarbiavimo sistemos dažnai yra fragmentiškos ir neišsamios, todėl dar labiau apsunkina veiksmingą tokių duomenų gavimą. Dėl to valdžios institucijoms dažnai būna sunku arba net neįmanoma pasiekti vieno iš pagrindinių baudžiamojo proceso tikslų - nustatyti ir nuteisti nusikaltėlį. Deja, šie klausimai nėra plačiai aptariami, nors jie labai svarbūs praktikai.

Šio straipsnio tikslas - visų pirma apžvelgti, kaip autorius apibrėžia skaitmeninių duomenų sąvoką ir kaip ji susijusi su skaitmeniniais duomenimis ir elektroniniais (arba skaitmeniniais) įrodymais. Taip pat bus pateikti specifiniai skaitmeninių duomenų bruožai, kurie aiškiai skiria juos nuo kitų įrodymų šaltinių, kurie gali būti naudojami baudžiamajame procese. Toliau, remiantis Europos Sąjungos pavyzdžiu, bus aptarta skaitmeninių duomenų svarba baudžiamajam procesui, taip pat aptarti skaitmeninių duomenų gavimo kanalai ir nurodyti jų trūkumai, turintys įtakos galimybei juos veiksmingai gauti. Taip pat bus atkreiptas dėmesys į tai, kaip sunkumai veiksmingai gauti skaitmeninius duomenis veikia tolesnio tokio proceso vykdymo galimybes. Galiausiai, bus aptarti veiksmai, kurių ėmėsi Europos Sąjunga ir Europos Taryba, siekdamos išspręsti esamas skaitmeninių duomenų gavimo problemas, ir palyginti atrinkti konkretūs klausimai, susiję su anksčiau minėtų subjektų priimtais teisės aktais.

Šis straipsnis dėl plačios ir įvairiapusės aptariamos temos apimties negali būti laikomas išsamiu šio klausimo tyrimu. Tačiau tai yra glaustas įvadas į pirmiau minėtas problemas.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 1 (29), 2024, p. 3-24

RAKTINIAI ŽODŽIAI

Skaitmeniniai duomenys, tarpvalstybinis duomenų gavimas, tiesioginė prieiga, teisminis bendradarbiavimas, tiesioginis bendradarbiavimas