Paweł Olber[1]
ORCID: 0000–0002–4614–9527

Obtaining data located in devices or IT systems — selected issues in light of the provisions of criminal procedural law

The diversity of opinions and beliefs of representatives of national law enforcement authorities on the subject of procedural practice related to obtaining data contained in devices or IT systems for evidential purposes contributed to the adoption of a position by the National Prosecutor's Office. The view of the National Public Prosecutor's Office was presented in a letter of 25 July 2018[2].

However, before the position of the National Public Prosecutor's Office is presented, it should be mentioned that a practical discourse in the field of procedural protection of digital evidence was conducted, *inter alia*, through a discussion forum of the Polish Public Prosecutors, where a dialogue was undertaken on the admissibility of carrying out a search of an e-mail box, as well as a thread relating to the procedural activity relevant to the search for digital evidence[3].

[1] Lt. dr Paweł Olber - senior lecturer at the Police Academy in Szczytno. The author's interests include forensic computer science, in particular, research on digital evidence and issues related to the legal and technical aspects of computer data security, as well as issues of combating cybercrime.

Contact the author through the editorial office.

[2] Letter PK II P 073.81.2016. The full text of the standpoint of the National Public Prosecutor›s Office can be found in the Electronic Register of Investigative Activities (ERCDŚ) in the tab 'Litigation Essentials'. The application is available through the Police Data Transmission Network (PSTD) in every unit and organisational unit of the police in the country.

[3] On the discussion forum of the Polish prosecutors available (after logging into the website: *Electronic source*: www.prokuratorzy.net/index.php, *accessed*: 2 July 2019, it is required to set up an account) there is, among others, a thread about mobile phones, the title of which is also a question: 'Inspection or search of a mobile phone?' Among many entries, you will find a longer conversation, of which the following is a fragment:

'When searching a suspect, for example, the evidence is secured, for example, by telephone. The secured evidence is then inspected. Thus, the examination of the contents of the phone (and possibly also the copying of the phone) is recorded in the inspection protocol, not in the search protocol. The same is true

Another example of an exchange of views and opinions on the process of obtaining digital evidence is a discussion conducted in the 'Police 997' magazine, concerning the possibility of accessing evidence stored in the memory of devices containing IT data, which was devoted to IT system searches and inspections[4].

It is important to stress that any discussion on the possibilities of accessing IT data stored in devices' memory and IT systems should be evaluated positively, especially as law enforcement and judicial authorities are obliged to constantly supplement and broaden their knowledge on methods of securing evidence. It is also obvious that although the above statement is valid on the grounds of the completely evidentiary proceedings, it refers mainly to forensic computer science, which is a dynamically developing field[5]. The proper securing of digital evidence, both from a technical and procedural point of view, is one of the components that influences its evidential value[6]. Any failure and negligence in this respect leads to a loss of credibility and authenticity of the secured digital evidence, and consequently to a loss of its evidential value[7].

---

with computers and stuff. Different views are wrong (except that they are not pragmatic)'.

In the case of a different view, there would be a 'search' of the item that was secured during the search.

'Let me be clear: The telephone as an item is subject to inspection, but access to the IT data contained in it (a device containing IT data) is only possible through a search. Because why was it introduced into the Code of Criminal Procedure? In 2003, the provision of Article 236a [...]. Since that change, a search is a procedural activity whose purpose is to detect (find) persons or items, as well as to obtain specific data to which a room, item, person, place and device containing IT data, as well as an IT system, may be subjected. A search of a device or IT system is intended to find specific IT data. These data must be of such a kind that they may constitute evidence in a case or are subject to seizure in the course of criminal proceedings. The provision (search warrant) cannot be limited to a laconic statement that it is intended to 'find information', but must be individualised'.

'[...] We traditionally do a phone check and nobody thinks about it. The same applies to the appointment of experts to review the data saved and deleted. But it should be a proper search to get to the data'.

'[...] So, the search is clear [...] Good to know'.

'Clearly [...] visual inspection. Neither 236a nor 205 the Code of Criminal Procedure indicate that a search is being performed'.

[4] Wiciak K, Kosiński J, Oglądamy czy przeszukujemy? Policja 997. *Electronic source*: http://www.gazeta.policja.pl/997/informacje/144955,Ogladamy-czy-przeszukujemy.html, *accessed*: 2 July 2019.

[5] Karasek P, Gdy dowodem są dane — czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych. *Edukacja Prawnicza, 2015, No. 2(158). Electronic source*: http://www.edukacjaprawnicza.pl/gdy-dowodem-sa-dane-czyli-prawdy-i-mity-zwiazane-z-pozyskiwaniem-dowodow-cyfrowych/, *accessed*: 2 July 2019.

[6] *Ibid.*

[7] *Ibid.*

Legal background to the considerations

The diversity of opinions of representatives of national law enforcement agencies on the subject of the process of obtaining data contained in the devices or information systems is related to Article 236a of the Code of Criminal Procedure[8], which states that the provisions of Chapter 25 shall apply respectively to the owner and user of a device containing computer data or an information system in respect of the data stored in that device or system or on a medium at its disposal or use, including correspondence sent by e-mail.

Process steps in the form of IT data retention and IT system searches were established in the Polish criminal procedure as a result of the amendment of 10 January 2003. The amendment introduced to the Act of 6 June 1997 – the Code of Criminal Procedure, the provision of Article 236a, which provides for appropriate application of the provisions of Chapter 25 of the Code of Criminal Procedure concerning the administrator and user of the information system. This provision was modified by the Act of 18 March 2004 amending the Act – the Code of Criminal Procedure, and the Act – the Code of Offences. As a result of the amendment, Article 236a of the Code of Criminal Procedure received new wording, which is unchanged until now[9].

In the new wording, the scope of application of Article 236a of the Code of Criminal Procedure has been extended to devices containing IT data. The introduced change provides more possibilities to search for IT data as it allows any device containing such data to be searched, and not only the data carrier itself, available through the IT system.

The provision of Article 236a of the Code of Criminal Procedure is the expression of the implementation of the Council of Europe Convention on Cybercrime, which was drawn up in Budapest on 23 November 2001, into Polish law[10]. The obligation to ensure that the parties can carry out activities concerning IT systems and the stored data results from the assumption that traditional ways of obtaining evidence are inappropriate as far as computer equipment and digital data are concerned. The application of traditional procedural rules on searches and seizures is not sufficient when acquiring information stored in information systems or on data carriers. Existing solutions in the Polish legal system were focused on IT systems and data carriers as well as on mobile items, while the most important are the recorded information and data[11].

[8] *Ibid.*

[9] Ustawa z 10 stycznia 2003 r. o zmianie ustawy — Kodeks postępowania karnego, ustawy — Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (DzU z 2003, nr 17, poz. 155).

[10] *Ibid.*

[11] *Ibid.*

The provision of Article 236a of the Code of Criminal Procedure refers to an IT system and a device containing IT data. These terms are not defined in Polish criminal law. For definitions of these terms, see the Council of Europe Convention on Cybercrime, according to which:

— 'Computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including the appropriate software program for the performance of functions by an information system. (Article 1(b)).
— 'Information system' means any device or group of interconnected or related devices, one or more of which, according to the programme, perform automatic data processing. (Article 1(a)).

IT data are also stored in the subscriber's terminal equipment, as provided for in Article 173(1) of the Telecommunications Law, and therefore Article 236a of the Code of Criminal Procedure constitutes the basis for the analysis of the memory content of mobile devices as part of a search.

The abovementioned notion of IT data includes the term 'in a form suitable for processing', which means that IT data may be processed directly by an IT system. Computer data must be understood as data in digital form or any other directly processable form[12].

The Council of Europe Convention on Cybercrime also contains a definition of 'traffic data', which is a category of IT data. Traffic data shall mean any information technology data relating to communication through an information system, generated by an information system that has formed a part in a communication chain, indicating its origin, destination, path, time, date, size, duration, or type of service concerned. Traffic data is generated by an information system and forms part of a communication chain to convey communication from its source location to the destination. This data is ancillary to the message itself. In the case of offences committed via the Internet, traffic data is needed to determine the source of the message as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data belongs to the category of fugitive data, so it is necessary to order its prompt protection. The collection of traffic data is considered less intrusive as this information does not reveal the content of the messages transmitted. Traffic data includes the following categories of information: a source of connection (transfer), destination, route, time, date, duration, and type of service. Not all of the categories presented will always be technically available or secure by the service provider. A call source refers to a telephone number, IP address, or similar identification of a piece of telecommunications equipment. The term 'destination' refers to the indication of the device to which the messages are transmitted. The term 'type of service' refers to the type of service used on the Internet, such as file transfer, e-mail or instant messaging[13].

[12] The explanatory report to the Council of Europe Convention on cybercrime, point 25. *Electronic souce*: https://rm.coe.int/16800cce5b, *accessed*: 4 July 2019.

[13] *Ibid.,* points 28-31.

In turn, the term 'device' should be understood as an object which enables the realisation of a specific process or an assembly of interconnected elements forming a functional whole, having a strictly defined form of construction depending on the operating parameters and purpose. In such a concept, they include devices such as the already-mentioned mobile devices. The term 'holder' should be understood as a person authorised to dispose of the system, having the system at its disposal and disposing of it at their discretion. Therefore, the person in charge will be the system owner or administrator. The 'user', on the other hand, is the person using and operating the system. For example, a user will be the owner of an e-mail account[14].

Retention of IT data, devices and media

According to Article 217(1) of the Code of Criminal Procedure, law enforcement and judicial authorities may retain items. The retention may be carried out by voluntary handover of the items or, in the case of refusal to hand them over voluntarily, by forced withdrawal. The legislator also allows for the retention of IT data or devices and media containing such data (Article 217(1) and (5) of the Code of Criminal Procedure in connection with Article 236a of the Code of Criminal Procedure). In a situation where the mentioned activity aims at obtaining IT data, the response to the request for data may be interpreted as a voluntary indication of the location of such data in the IT system, on the carrier, or in the device. In the case of voluntary data handover, the search should not be continued[15]. In the context of the above statements, it is worth emphasising that access to data should be understood as providing an opportunity to read the information or to take possession of the information carrier, including the copying of the information[16].

IT data in respect of which a request for handing over has been made, does not have to be located at the person's location, so for example at home, at school, at work, etc. It is enough that this data will be within the range of a given person, who will be able to pass it to representatives of law enforcement agencies e.g. through copying, sending, etc. The data does not have to be located on the territory of Poland; it may be, for instance, e-mail files located in a mailbox on a foreign e-mail server[17], data

[14] Skorupka J (Ed.), Kodeks postępowania karnego. Komentarz. Warsaw, 2018.

[15] Wojtuszek R, Procesowy aspekt zwalczania cyberprzestępczości. *Kwartalnik Policyjny,* 2017, No. 4, p. 84.

[16] Wyrok SO Warszawa–Praga w Warszawie z 8 maja 2017, sygn. VI Ka 1461/16. *Electronic source*:orzeczenia.warszawapraga.so.gov.pl/content/$N/154510000003006_VI_Ka_001461_2016_Uz_2017-05-08_001, *accessed*: 10 July 2019.

[17] Wyrok SO Warszawa–Praga w Warszawie z 8 maja 2017, sygn. VI Ka 1461/16. *Electronic source*:orzeczenia.warszawapraga.so.gov.pl/content/$N/154510000003006_VI_Ka_001461_2016_Uz_2017-05-08_001, *accessed*: on 10 July 2019.

located on a virtual hard disk or available via an IT system. If a request for specific IT data is met by indicating it and making it available by the user or the person in charge (usually after logging in to a given IT system or resource), the law enforcement authorities may retain the data independently by copying it to an external carrier, which will then be secured.

Search of a carrier, device or IT system

It is also possible to search the data carrier, device, or information system (Article 219 in connection with Article 236a of the Code of Criminal Procedure). The mentioned activity may take the form of a search in the IT system or medium and a search in specific resources. It is indicated in the relevant literature that typical activities of the data search include searching for specific phrases, reading data, as well as checking and reviewing specific resources[18].

It seems that in the event of a necessity to retain data and to search the contents of a device, in particular, a mobile device or an IT system, this activity (from a technical point of view) should be carried out by an officer of the Bureau for Combating Cybercrime at the National Police Headquarters, or of the department for combating cybercrime at the relevant police headquarters, an expert in the field of IT research, as well as an expert or certified specialist in the field of digital media research at police forensic laboratories.

The validity of the above statement results from the complexity of the abovementioned activities, as well as from the necessity to have knowledge in the field of specialist software operations, and the construction and operation of IT systems. Moreover, assistance in planning, preparation, and implementation of cases where knowledge and skills related to advanced technical solutions are required is included in the scope of the tasks of departments for combating cybercrime[19]. Exploring the data manually, which does not require specialist knowledge, can lead to the misconception of checking the content of the entire carrier. Therefore, in most cases, additional software will need to be used to define the search criteria, for example by entering a list of phrases to be searched, and specifying the file formats that will be included in the search. However, regardless of how the search is performed, one should be aware that the search activity will never include all of the data that is analysed during forensic examinations performed by experts and concluded in their opinion[20]. An inseparable

[18] Wojtuszek R, Procesowy..., *op. cit.,* p. 84.

[19] Tasks carried out by the Department of Cybercrime at the Regional Police Headquarters in Bydgoszcz. *Electronic source*: http://bip.bydgoszcz.kwp.policja.gov.pl/KWB/wolnytekst/20180,dok.html, *accessed*: 10 July 2019.

[20] Department for Research on Documents and Audio-Visual Technology CLKP. *Electronic source: http://clk.policja.pl/clk/clkp /struktura/*zaklad-badan-dokumento/65246,Zespol-Badan-Dokumentow-Audiowizualnych.html, *accessed*: 10 July 2019.

element of IT research is the recovery of data that has been previously deleted by the user of a given device or IT system.

In the context of performing a search of an IT device or system, the regulations contained in Article 220(3) of the Code of Criminal Procedure are important concerning urgent cases. The situations in which law enforcement agencies find that switching off a device may cause permanent data loss should be considered to be urgent when searching for devices (e.g. mobile phones and smartphones) and information systems. Such a circumstance may occur, for example, in the case of encrypted data, available during a given activity. In such a situation, switching off a given device will cause permanent data loss.

In urgent cases, the searching authority shall be required to produce an order from the head of its unit or a service card. A search conducted in this way must be approved immediately by the court or prosecutor. The searching authority is obliged to inform the person concerned of the possibility to request the court or prosecutor's approval. Such a decision should be delivered to the person within 7 days from the date of the action (Article 220(3) of the Code of Criminal Procedure).

Searches shall only be admissible within the scope of the system of which the person is the owner or user. The Polish legislator has not implemented regulations allowing for remote searches via the Internet. In the event of such a necessity, it is necessary to perform a search conducted simultaneously in several places[21].

The above provisions have raised many doubts as to the indication of the process step appropriate to obtain the data stored in the memory of mobile phones, an example of which is (mentioned at the beginning of the article) a polemic conducted in the 'Police 997' monthly. In their practice to date, investigators were acquainted with the content of IT devices and mobile phones in the course of visual inspection, of which a relevant protocol was drawn up, according to Article 143(1) point 3 of the Code of Criminal Procedure and Article 207 of the Code of Criminal Procedure.

Inspection of items

Visual examination is a set of forensic-procedural activities aimed at disclosing and securing material relating to a committed crime. According to Article 207(1) of the Code of Criminal Procedure and Article 209(1) of the Code of Criminal Procedure, if necessary, a person, items, and corpses may be inspected, which in such a situation are subject to detailed and comprehensive observation. However, the inspection is not always limited only to planned and detailed observations, because sometimes it can turn into real scientific and technical research[22].

[21] Lach A, Gromadzenie..., *op. cit.,* p. 23.

[22] Witkowska K, Oględziny. Aspekty procesowe i kryminalistyczne. Warsaw, 2013, pp. 13–14.

The purpose of the inspection is to clarify the nature and circumstances of the event and to gather factual evidence. The purpose of the inspection is achieved by recording the look and condition of the items and, above all, by documenting the location of the traces[23]. Every carrier of traces of the crime revealed at the scene of the incident, and every item found or issued in the course of a search of the place, room or person and the retention of items shall be inspected. Among the most important and usually first sources of information about the crime is the visual inspection of the place where the crime was committed, which is usually combined with the visual inspection of items. In the course of the examination of items, their external characteristics are examined[24]. This position is also shared by Tomasz Grzegorczyk, according to whom the examination 'involves examining the evidence that is the item, as well as the document, if we are interested in its physical characteristics and not its intellectual content'[25]. The examination shall be carried out exclusively by the procedural authority, which may call upon an expert (Article 198(1) of the Code of Criminal Procedure), or a specialist (205(1) of the Code of Criminal Procedure)[26].

Considering the above, one fundamental question arises as to which of the abovementioned process stages is appropriate for obtaining data located in the memory of IT devices.

The Criminal Bureau at the National Police Headquarters considered a search of a device (mobile phone) to reveal specific IT data to be the correct action. The justification of the adopted position indicated that access to data stored in the memory of a mobile phone constitutes a serious interference in the person's informational autonomy expressed in Article 51 paragraph 2 of the Constitution of the Republic of Poland; therefore, access to data is possible through a search, not through a visual inspection. It was emphasised that the purpose of a search should be to disclose strictly defined IT data, which may constitute evidence in a case, or be subject to seizure in criminal proceedings[27].

In response to this position, a different view was presented, which shows that the proper procedural stage in this respect is a visual inspection. It was considered that this should be preferred, in particular during

[23] Jerzewska J, Od oględzin do opinii biegłego. Poradnik dla prowadzącego postępowanie karne. Warsaw, 2010, p. 14.

[24] Bieńkowska B et all, Wykład prawa karnego procesowego. Białystok, 2012, p. 248.

[25] Grzegorczyk T, Kodeks postępowania karnego oraz ustawa o świadku koronnym. Warsaw, 2008, p. 480.

[26] Wyrok SN z 3 października 2006, sygn. IV KK 209/06, p. 5. *Electronic source*: http://sn.pl/sites/orzecznictwo/Orzeczenia1/IV%20KK%20209-06.pdf, accessed: 10 July 2019.

[27] Wojtuszek R, Telefon komórkowy. Oglądamy czy przeszukujemy? *Electronic source*: http://gazeta.policja.pl/997/ archiwum-1/ 2017 /numer-142-012017/137717,Telefon-komorkowy.html, *accessed*: 11 July 2019.

the initial period of proceedings and in the context of a high sensitivity of digital data to the possibility of irretrievable loss[28].

However, Marek Chrabkowski does not agree with this view, claiming that the inspection is not subject to judicial or prosecutorial control, and in chapter 23 of the Code of Criminal Procedure concerning visual inspections, the opening of corpses and trial experiments, there is no reference to the procedure in the case of disclosure of data protected by telecommunication secrecy[29], which includes text messages.

It seems that the opinion of the National Public Prosecutor's Office on the procedural practice related to obtaining IT data contained in devices or IT systems for evidential purposes may be a compromise in this respect.

Opinion of the National Public Prosecutor's Office

The National Public Prosecutor's Office allows two 'methods' of obtaining the information contained in devices or systems containing IT data for criminal proceedings. Obtaining IT data is possible mainly through searching the device or system. It is also possible to obtain IT data in the course of the search, if the device containing the data was placed at the disposal of a law enforcement authority and its owner or user has been provided with procedural guarantees provided for by the provisions of the Code of Criminal Procedure.

Following the opinion of the National Public Prosecutor's Office, if a request for the release of data stored in a device or system by the person in charge or the user is not aimed at depriving the person in charge/user of access to the data and to the device itself, this activity should be limited to the request to make and release an electronic copy of the data. This request should be indicated in the decision of the court or prosecutor. Due to a specific nature of IT data, its retention may consist of copying. Each time it should be assessed whether a given device will be necessary for the further course of proceedings. If there is no need to retain the device, then it shall be sufficient to retain the IT data based on the decision issued according to Article 217(1) of the Code of Criminal Procedure, or Article 220(1) of the Code of Criminal Procedure in connection with Article 236a of the Code of Criminal Procedure. However, it is not a mistake to issue a decision on the retention of items in the form of IT/mobile equipment and the data contained therein. However, in this case, the legal basis should also be Article 236a of the Code of Criminal Procedure, and the acquaintance with the contents of the telephone should be carried out in the form of a search.

The National Public Prosecutor's Office also refers to the situation of acquaintance with the contents of the device due to the device itself being

[28] Wiciak K, Kosiński J, Oglądamy..., *op. cit.*

[29] *Ibid.*

legally at the disposal of a police officer, i.e. it was issued under Article 217 of the Code of Criminal Procedure, or found during a search under Article 219 of the Code of Criminal Procedure. In such a situation (according to the opinion of the National Public Prosecutor's Office), to become acquainted with the contents of the device, it will be sufficient to carry out an inspection.

In the quoted opinion of the National Public Prosecutor's Office (to the extent related to the inspection activities), selected views (or rather fragments thereof) represented in the legal literature were cited. An example is Krystyna Witkowska's view, according to which the purpose of the inspection is to identify and establish traces related to the event, as well as to determine the specific features of an item or its content[30]. Krystyna Witkowska gives concrete examples (which are not indicated by the National Prosecutor's Office), specifying that, among others, checking the content of items can refer to checking the interior of a safe. Next, Krystyna Witkowska does not make any deliberations related to the specification of the content of items, but explains that during the inspection, only their external features can be found, which include colour, shape, size, consistency, markings, damage and surface structure[31].

The next view cited by the prosecution is similar, which is as follows: 'An electronic record takes […] the attributes of factual evidence when it can be attributed the meaning of a «trace» of the deed accused, even if that «trace» has a conceptual content. […] Then the information content of such evidence (source of evidence) is extracted through an examination (irrespective of whether the record is subject to an expert's report if the need arises)'[32]. The fragment quoted in this opinion by Dorota Karczmarska comes from a review of a book by Arkadiusz Lach, entitled *Dowody elektroniczne w procesie karnym*[33] [*Electronic evidence in a criminal trial*, rm]. The author of the review does not fully share A. Lach's opinion that electronic evidence should be classified as material evidence. Justifying her view, Dorota Karczmarska refers to the electronic record, stating that the extraction of the information content from such evidence takes place through visual inspection. It should be stressed that this is a single statement which was formulated as part of deliberations on the recognition of electronic evidence as evidence in kind, and not in the context of decisions made in the context of a procedural activity appropriate for obtaining data located in devices or IT systems.

[30] Stanowisko Prokuratury Krajowej z 25 lipca 2018 r., PK II P 073.81.2016, p. 7.

[31] Witkowska K, Procesowe i kryminalistyczne aspekty oględzin rzeczy w postępowaniu karnym. *Prokuratura i Prawo,* 2011, No. 1, p. 102.

[32] Stanowisko Prokuratury Krajowej z 25 lipca 2018 r. …, *op. cit.,* p. 7.

[33] Karczmarska D, Dowody elektroniczne w procesie karnym TNOiK, Arkadiusz Lach Toruń 2004:[review]. *Palestra*, 2006, No. 51/5–6. *Electronic source*: http://bazhum.muzhp.pl/media//files/Palestra/Palestra-r2006-t51-n5_6(581_582)/Palestra-r2006-t51-n5_6(581_582)-s265-268/Palestra-r2006-t51-n5_6(581_582)-s265-268.pdf, *accessed*: 12 July 2019.

Summary

Taking into account the position of the National Public Prosecutor's Office, it should be stated that the priority of representatives of national law enforcement bodies and the judiciary in terms of obtaining data should be to retain it by copying specific files or contents. If, in the course of proceedings, it is possible to establish that a given person's device may contain information which is important and significant for the objectives of criminal proceedings, then a police officer should apply to the prosecutor for a decision according to Article 217(1) of the Code of Criminal Procedure, or Article 220(1) of the Code of Criminal Procedure in connection with Article 236a of the Code of Criminal Procedure, and then check the contents of the device as part of a search of the IT system[34].

In this respect, however, some doubts and questions may arise, including how the authority empowered to require the person in charge or the user to issue data will verify that he or she has obtained all IT data which is relevant in the proceedings, as well as how a police officer will be able to establish that there is relevant information included a particular device. It seems that establishing the above issues is the purpose of the IT system search, and will not be possible without checking or reading the content of the device within the framework of process activity. Moreover, it should be emphasised that the activity of searching the IT system should be performed in the presence of the owner or authorised officer of the device who has certain procedural rights.

Another solution indicated by the National Public Prosecutor's Office concerns a situation in which the device was lawfully placed at the disposal of a police officer, e.g. after a prior decision to demand that the item be released, or it is found in the course of a room search. In such circumstances, the National Public Prosecutor's Office considers it sufficient to carry out an inspection aimed at familiarising oneself with the contents of the device.

However, regarding the position of the National Public Prosecutor's Office, it should be stressed that it is certainly helpful in interpreting the rules on the process of obtaining data located in devices or IT systems. However, this position cannot be considered a final one — it is advisable to reflect further on the appropriate legal solutions to facilitate effective and lawful acquisition and securing of digital traces, thus fulfilling the obligation to gather knowledge on the best methods of securing evidence by law enforcement and judicial authorities.

The position of the National Public Prosecutor's Office does not take into account, in particular, legal aspects related to gaining access to the content of telecommunication transmissions in, among others, the form of text messages protected by telecommunications confidentiality. In particular, this applies to visual inspection activities which are excluded from

[34] Stanowisko Prokuratury Krajowej z 25 lipca 2018 r. ..., *op. cit.,* p. 4.

a priori prosecutorial and court control[35], and within which unlimited access to data stored in the memory of mobile devices is obtained, including the content of electronic correspondence. In investigative practice, the exploration of the content of mobile devices within the framework of visual inspection is carried out, as a rule, by manual checking of the memory content of devices launched together with original SIM cards and memory cards (if they are installed)[36]. This method of operation does not protect the data against alteration, jeopardising its evidentiary value, and entails the risk of omitting or deleting relevant content. Such a procedure should be considered inappropriate, since it gives an incomplete picture of the actual content of the devices, based on which findings of fact are made, and thus the subject matter of the procedure is decided.

Certainly, the method of documenting process activities consisting in reading IT data from the memory of mobile devices and other carriers and IT systems should be supported by jury considerations[37]. However, it should be noted that forensic IT techniques should ensure the legal effectiveness of digital evidence by enabling it to be correctly read and secured[38]. However, such guarantees are not provided by the execution of the abovementioned activities within the framework of visual inspection carried out independently by police officers conducting initial investigations.

Technical considerations require that these activities shall be carried out by (or with the participation of) law enforcement officers with appropriate knowledge and qualifications, as well as with appropriate equipment and software. In the case of mobile devices, these activities should consist in reading the data after installing a specially prepared copy of the original SIM card that allows the device to be started up without the possibility of communication with the mobile network.

Taking into account the above, it should be concluded that gaining access to IT data located in the memory of devices and IT systems in the course of inspection activities raises doubts, as it gives law enforcement officers unlimited access to the content of the devices, and most phones/smartphones contain data legally protected by telecommunications secrecy. This view is also shared by Marek Chrabkowski who, referring to police practice in this respect, claims that the regulations governing the inspection of items do not contain any reference to the procedure to be followed in the case of disclosure of data protected by telecommunications confidentiality and do not comply with constitutional standards in the scope of sufficient specification of legal regulations which interfere with human rights and freedoms[39].

Therefore, it seems that the acquisition of IT data should be carried out primarily at the place of the incident, with the use of specialised software intended for this purpose, as part of a search of the device, carrier

[35] Stanowisko Prokuratury Krajowej z 25 lipca 2018 r. …, *op. cit.,* p. 4.

[36] This statement applies to police officers conducting initial investigations.

[37] Stanowisko Prokuratury Krajowej z 25 lipca 2018 r. …, *op. cit.,* p. 4.

[38] Karasek P, Gdy dowodem…, *op. cit.*

[39] Chrabkowski M, Dostęp…, *op. cit.,* p. 59.

or IT system, as well as within the framework of forensic examination in a situation where the device was acquired under Article 217 of the Code of Criminal Procedure, or Article 220 of the Code of Criminal Procedure, and is at the disposal of law enforcement authorities. However, the possibility of obtaining IT data within the framework of visual inspection cannot be completely excluded, only concerning devices for which there is not a justified suspicion that they may contain classified information (letters or other documents) of a personal nature, information covered by professional secrecy or another legally protected secrecy[40]. In such situations, however, a specialist referred to in Article 205 of the Code of Criminal Procedure should participate in the visual inspection. The participation of a specialist[41] in the inspection may consist in the provision and maintenance of dedicated software and hardware, e.g. a so-called data recording blocker — a device protecting the carrier against any data modifications. M. Chrabkowski rightly pointed out that in the case of an inspection, there is no statutory procedure in the situation of disclosure of data protected by telecommunications confidentiality, however, this procedure has been defined (similarly as in the case of classified information, information covered by professional or other legally protected secrecy, as well as letters or other documents of a personal nature) in the methodology of the Central Police Forensic Laboratory, entitled *Zabezpieczanie śladów cyfrowych*, [*Digital trace retention, rm*], published on 25 April 2019[42]. This document is intended for all representatives of national law enforcement and judicial authorities who undertake to preserve digital evidence. In particular, it is addressed to officers and civil employees of the police acting as specialists within the meaning of Article 205 of the Code of Criminal Procedure, employees and officers of the Cybercrime Bureau/departments, as well as experts in the field of IT research and experts and certified specialists in the field of digital carrier research of police forensic laboratories.

Obtaining information on private lives of individuals by public authorities must be limited to necessary situations, which are permissible in a democratic state solely to protect constitutionally recognised values, and following the principle of proportionality. The conditions under which such data is collected and processed must be standardised and transparent, in a way that excludes arbitrariness and discretionary use[43]. It is, therefore, necessary to introduce appropriate statutory regulations containing conditions for access to equipment containing IT data, included

[40] The catalogue of these devices does not include the mobile phones/smartphones in use, because (obviously) every mobile phone/smartphone in use contains legally protected data.

[41] The catalogue of these devices does not include the mobile phones/smartphones in use, because (obviously) every mobile phone/smartphone in use contains legally protected data.

[42] The methodology of securing digital evidence by the Police Central Forensic Laboratory can be made available only upon request of the court or prosecutor's office.

[43] Wyrok TK z 30 lipca 2014, sygn. K 23/11 (DzU z 2014, poz. 1055), p. 56.

in the framework of visual inspection activities. To a certain extent, these issues are regulated by the aforementioned methodology for securing digital traces, owned by the Police Central Forensic Laboratory. However, regardless of the creation of the document in question, one should support the *de lege ferenda* postulate, introduced by the legislator[44]:

— a prior judicial review allowing interference by the procedural authorities with data protected by telecommunications secrecy;
— a catalogue of offences, the commission of which would justify such interference;
— a limited number of persons entitled to be acquainted with the contents of the transmissions stored in the terminal device;
— a specific procedure for all stored data terminal equipment regardless of the entity from which the evidence is secured.

References

Publications

Bieńkowska B et al, *Wykład prawa karnego procesowego*. Białystok, 2012.

Chrabkowski M, Dostęp do treści korespondencji SMS-owej w telefonie zabezpieczonym na potrzeby sprawy karnej. *Studia Iuridica Toruniensia*, 2018, Vol. XXII.

Grzegorczyk T, Kodeks postępowania karnego oraz ustawa o świadku koronnym. Warsaw, 2008.

Grzeszczyk W, Zmiany prawa karnego wprowadzone ustawą z dnia 18 marca 2004. *Prokuratura i Prawo*, 2004, No. 7–8.

Jerzewska J, Od oględzin do opinii biegłego. Poradnik dla prowadzącego postępowanie karne. Warsaw, 2010.

Karczmarska D, Dowody elektroniczne w procesie karnym TNOiK, Arkadiusz Lach Toruń 2004:[review]. *Palestra*, 2006, No. 5–6.

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

Moszczyński J, Subiektywizm w badaniach kryminalistycznych. Przyczyny i zakres stosowania subiektywnych ocen w wybranych metodach identyfikacji człowieka. Olsztyn, 2011.

Skorupka J (Ed.), Kodeks postępowania karnego. Komentarz. Warsaw, 2018.

Witkowska K, Oględziny. Aspekty procesowe i kryminalistyczne. Warsaw, 2013.

Witkowska K, Procesowe i kryminalistyczne aspekty oględzin rzeczy w postępowaniu karnym. *Prokuratura i Prawo*, 2011, No. 1.

Wojtuszek R, Procesowy aspekt zwalczania cyberprzestępczości. *Kwartalnik Policyjny*, 2017, No. 4.

[44] Chrabkowski M, Dostęp..., *op. cit.,* p. 59.

Legal acts

Ustawa z 6 czerwca 1997 — Kodeks postępowania karnego (DzU z 2018, poz. 1987).

Ustawa z 10 stycznia 2003 o zmianie ustawy — Kodeks postępowania karnego, ustawy — Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (DzU z 2003, nr 17, poz. 155).

Konwencji Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie 23 listopada 2001 (DzU z 2015, poz. 728).

Other sorces

Electronic source: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_%20auth=Vhy0xRnS, *accessed*: 3 July 2019.

Electronic source: www.prokuratorzy.net/index.php.

Karasek P, Gdy dowodem są dane — czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych. *Edukacja Prawnicza*, 2015, No. 2(158). *Electronic source*: http://www.edukacjaprawnicza.pl/gdy-dowodem-sa-dane-czyli-prawdy-i-mity-zwiazane-z-pozyskiwaniem-dowodow-cyfrowych/, *accessed*: 2 July 2019.

Karczmarska D, Dowody elektroniczne w procesie karnym TNOiK, Arkadiusz Lach Toruń 2004:[recenzja]. *Electronic source*: http://bazhum.muzhp.pl/media//files/Palestra/Palestra-r2006-t51-n5_6(581_582)/Palestra-r2006-t51-n5_6(581_582)-s265-268/Palestra-r2006-t51-n5_6(581_582)-s265-268.pdf.

Pismo Prokuratury Krajowej z 25 lipca 2018 PK II 073.81.2016.

Raport wyjaśniający do Konwencji Rady Europy o cyberprzestępczości. *Electronic source*: https://rm.coe.int/16800cce5b, *accessed*: 4 July 2019.

Stanowisko Prokuratury Krajowej z 25 lipca 2018 PK II P 073.81.2016.

Wiciak K, Kosiński J, Oglądamy czy przeszukujemy? Policja 997. *Electronic source*: http://www.gazeta.policja.pl/997/informacje/144955,Ogladamy-czy-przeszukujemy.html, *accessed*: 2 July 2019.

Wojtuszek R, Telefon komórkowy. Oglądamy czy przeszukujemy? *Electronic source:* http://gazeta.policja.pl/997/ archiwum-1/ 2017 /numer-142-012017/137717,Telefon-komorkowy.html, *accessed*: 11 July 2019.

Wyrok SN z 20 czerwca 2013 sygn. III KK 12/13. *Electronic source*: http://www.sn.pl/sites/orzecznictwo/Orzeczenia3/III%20KK%2012-13.pdf.

Wyrok SN z 3 października 2006 sygn. IV KK 209/06. *Electronic source*: http://sn.pl/sites/orzecznictwo/Orzeczenia1/IV%20KK%20209-06.pdf.

Wyrok SO Warszawa–Praga w Warszawie z 8 maja 2017 sygn. VI Ka 1461/16. *Electronic source*: orzeczenia.warszawapraga.so.gov.

pl/content/$N/154510000003006_VI_Ka_001461_2016_Uz_2017-05-08_001, *accessed*: 10 July 2019.
Wyrok TK z 30 lipca 2014 sygn. K 23/11 (DzU z 2014 r., poz. 1055).
Tasks implemented by the Department for Combating Cybercrime of the Regional Police Headquarters in Bydgoszcz. *Electronic source*: http://bip.bydgoszcz.kwp.policja.gov.pl/KWB/wolnytekst/20180,dok.html, accessed: 10 July 2019.
Department for Research on Documents and Audio-visual Technology CLKP. *Electronic source*: http://clk.policja.pl/clk/clkp /struktura/zaklad-badan-dokumento/65246, Zespol-Badan-Dokumentow-Audio-wizualnych.html, *accessed*:10 July 2019.

DOI: 10.5604/01.3001.0014.1139
http://dx.doi.org/10.5604/01.3001.0014.1139

Keywords: computer forensics, digital evidence, obtaining IT data, searching the IT system, device inspection, telecommunications confidentiality

Summary: There is a lack of consensus among national law enforcement and judicial authorities as to which procedural acts are relevant for obtaining data contained in devices or information systems for evidentiary purposes. It is easy to find supporters of the search of the information system as well as those who consider it appropriate to carry out inspections. However, regardless of many examples and arguments of various persons, it may seem that the compromise in this respect should be the position of the National Public Prosecutor's Office on the procedural practice related to obtaining data contained in IT equipment or systems for evidentiary purposes. However, the opinion of the National Prosecutor's Office does not take into account legally protected data, and in particular, legal aspects related to obtaining access to the content of telecommunications, including text messages protected by telecommunications secrecy. The article is a summary of the previous considerations regarding the possibility of obtaining data located in IT equipment or systems. The article also contains the author's conclusions, based on, inter alia, methodology for securing digital footprints, intended for all representatives of national law enforcement and judicial authorities.