PROF. DR. ERIKA RÓTH, EGYETEMI TANÁR
University of Miskolc | DOI: 10.32041/9788367149761/8

Chapter 8. Particulars of Evidence in Cybercrime Cases

8.1. Introduction

Introduction and analysis of the rules of evidence are very important if we deal with a special field of crime such as cybercrime. Before starting a detailed discussion of the topic, it should be noted, that there is no special procedural provision in this area regarding cybercrime in Hungary. The rules governing proceedings for all criminal cases must also be applied to cybercrime cases.

The other side of the phenomenon is, the "Evidence of cybercrime (…) differs from evidence of traditional crime. Accordingly, novel coercive measures, other investigatory powers, tactics, and technical methods are needed in order to secure evidence of cybercrime."[1] It follows from the nature of these offences, that certain means of evidence play significant role in this field such as physical evidence and electronic data. Employing a specialised expert is also often required in these cases.

But it is not only the specific means of evidence that need to be introduced. We have to speak about the method of obtaining it, since some of these means of evidence can be obtained by using covert means, e.g., secret surveillance of an information system. Due to the often cross-border nature of cybercrime, another important

[1] J. Riekkinen, *Evidence of cybercrime and coercive measures in Finland*, p. 1, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

issue is the acquisition of evidence in another country and the use of the obtained evidence. In this respect, judicial cooperation in criminal matters is of great importance.

In the beginning of this chapter, we intend to examine the general rules of evidence such as the lawfulness of evidence, evaluation of evidence etc. After that we will take a look at the means of evidence that can be used in Hungarian criminal proceedings. In the next part of the chapter specialities of evidence used in cybercrime cases and the specific problems of obtaining evidence will be discussed.

8.2. General Rules of Evidence

The effective Code of criminal procedure is Act XC of 2017 (hereinafter: HCCP) which entered into force on 1 July 2018. Regulation governing the use and evaluation of evidence in the Hungarian code on criminal procedure is based on the rules of the *free system of evidence*, since any means of evidence or evidentiary act specified in the Code may be used or applied freely in the criminal proceeding. The value of evidence is not determined in advance by law. The court, the prosecution service, and the investigating authority shall evaluate pieces of evidence freely both individually and in their totality, and it shall determine the result of the evidence according to its conviction thus formed. The only but very important limit is, that a fact originating from a means of evidence may not be taken into account as evidence if the court, the prosecution service, the investigating authority, or another authority acquired the given means of evidence by way of a criminal offence, a material violation of the procedural rights of a person participating in the criminal proceeding, or in any other prohibited manner (HCCP 167. §). But, in some respects, the Hungarian system of evidence is a so-called "mixed system"[2] as the law may order the use of certain means of evi-

[2] As Á. Farkas writes, this provision indicates the survival of certain elements of the legally bound system of evidence. Á. Farkas, E. Róth, *A büntetőeljárás*, Budapest 2018, p. 200. According to Mihály Tóth the current law is closer to the free evidentiary system, but its evidential system can actually be considered "mixed". E. Belovics, M. Tóth, *Büntető eljárásjog*, Budapest 2017, p. 146.

dence (HCCP 167. § (1) para.) and the manner of performing and conducting evidentiary acts, and examining and recording means of evidence may be specified by law (HCCP 166. § (2) para.).

With respect to the separation of procedural functions and the biding nature of the charge, it is very important that the prosecutor is responsible for discovering all facts required to prove the charge, and providing the evidence supporting them and making a motion to collect them. In the course of clarifying the facts of the case a court shall obtain evidence on the basis of motions. In the absence of a motion, the court is not obliged to obtain or examine any pieces of evidence (HCCP 164. §).

8.3. Means of Gathering Evidence

As it was mentioned earlier, the Hungarian system of evidence is (basically) free, but the HCCP provides a list of means of evidence and evidentiary acts. The free system of evidence means that any means of evidence or evidentiary act specified in the HCCP may be used or applied freely in the criminal proceeding. Means of evidence are the following:

a) witness testimony,
b) defendant testimony,
c) expert opinion,
d) opinion of a probation officer,
e) means of physical evidence, including documents and deeds, and
f) electronic data.

Although the enumerations of means of evidence is closed, the list is exhaustive, the enumeration of evidentiary acts in the HCCP appears to be exemplary (it is indicated by the term "in particular"), although we cannot mention any additional act that might be used in criminal proceedings. These acts are the following:

a) inspection,
b) on-site interrogation,
c) reconstruction of a criminal offence,

d) presentation for identification, confrontation,
e) and instrumental examination of a testimony.

In this subchapter we deal with means of evidence – except for expert opinion and electronic data which will be discussed in the next point – and with evidentiary acts, especially with rules of inspection, as it can be used in cybercrime cases quite frequently.

8.3.1. MEANS OF EVIDENCE

It is beyond dispute, that usually witness testimony and testimony of the accused could be a very important and frequently used means of evidence in criminal proceedings, in cybercrime cases the electronic data and expert opinion (of informatics/data science specialists) are of particular importance. Before dealing with these two means of evidence in details, we outline briefly the specific feature of other means of evidence.

Witness testimony is the most frequent evidence in criminal proceedings but in cybercrime cases it is less significant. Cybercrimes typically have no eyewitnesses,[3] but of course, the victim and anybody else who has knowledge of facts relevant to the offence can be interrogated as a witness. It is a civic duty to testify as a witness unless the HCCP makes an exception. These exceptions are regulated by the HCCP as the two main categories of obstacles to testifying: prohibition of giving testimony[4] and reasons of refusal to give testimony.

The *testimony of defendants*, especially if there is admission of guilt, may support the detection of an offence and the establishment of facts. In the Hungarian criminal procedure, the defendant is not obliged to testify and to tell the truth if he testifies, but he may not accuse falsely another person of having committed a criminal

[3] "Eyewitness and eyewitness testimonies and traditional physical evidence are rarely available." J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[4] The name of this category is misleading, because these persons shall not be interrogated, the addressees of the prohibition are authorities acting in the criminal proceedings.

offence, and he may not violate the right to respect for the deceased by stating any false fact (HCCP 185. § (1) para. d) point).[5]

It needs be said that the accused's confession can be the basis of several prosecutorial measures and decisions that can bring the proceeding to a conclusion favourable for the accused, such as mediation, conditional suspension of the proceeding, plea agreement, or in the case of accusation, the taking of measures necessary for quicker and simpler special procedures, such as (immediate) summary procedure or procedure for passing a penal order.

Physical evidence and *electronic data* are in very close connection with each other. In the former Code of criminal procedure, electronic data was one form of physical evidence. It was only created as a special means of evidence by the new Code. Even nowadays we can discover a connection among the rules concerning physical evidence when the legislator determines the definition of "document": a "document" is any physical evidence that records data by technical, chemical, or any other method, including, in particular, texts, drawings, and illustrations recorded in a paper-based form or as electronic data (HCCP 204. § (2) para.).

The *opinion of a probation officer* has a lesser importance in cybercrime cases. The opinion prepared by the probation officer describes the facts and circumstances characterising the personality and living conditions of the defendant, in particular his family situation, health, any addiction, housing situation, education, qualification, workplace or, in the absence of a workplace, data on

[5] Defendant shall be informed about his right concerning his testimony according to the 185. § (1) para. of the HCCP. Information concerns the following issues:

- he is not obliged to give a testimony; he may refuse to testify and to answer any question at any time during the interrogation; but he may decide to testify at any time, even if he refused to do so earlier,
- refusing to testify does not hinder the continuation of the proceeding or affect the right of the defendant to ask questions, make observations, or file motions,
- if he testifies, anything he says or makes available may be used as evidence,
- he may not accuse falsely another person of having committed a criminal offence, and he may not violate any right to respect for the deceased by stating any false fact.

his occupation, financial situation and assets; it shall also present any relationship between the discovered facts, circumstances, and the commission of the criminal offence, as well as the risk of reoffending, and the needs of the defendant. In the opinion, the probation officer provides information on employment possibilities that would be suitable for the defendant considering his skills, as well as healthcare and social care options available to him; he may suggest individual rules of behaviour or obligations to be imposed on a defendant, as well as interventions to be taken to mitigate the risk of reoffending (HCCP 203. § (1)–(2) para.). The probation officer's opinion can be helpful in determining the sanction by the court or discretionary measures taken by the public prosecutor, such as conditional suspension of the proceeding or referral of the case to a mediation procedure.

8.3.2. EVIDENTIARY ACTS

8.3.2.1. *Inspection*

The court, the prosecution service, or the investigating authority may order and carry out an inspection if a person, object, or site needs to be inspected, or an object or site needs to be observed to discover or establish a fact to be proven (HCCP 207. § (1) para.). During the inspection, means of physical evidence shall be sought and collected, and arrangements shall be made for the proper preservation of them.

In the course of an inspection, circumstances that are relevant to evidence shall be recorded in detail, in particular, the course, method, location, and condition of finding and collecting the inspection object. During the search for, recording, and securing of physical evidence, it is necessary to proceed in such a way that compliance with the rules of procedure can be verified subsequently. If possible and necessary, a visual, sound, or audio-visual recording, drawing or sketch shall be made of the object of the inspection, and it shall be attached to the minutes (HCCP 207. § (2) para.).

The HCCP allows the involvement of the expert during the inspection in all cases (HCCP 207. § (4) para.). This can be very important, since improper collection and recording of evidence can affect the success of the evidence. The participation of an *IT expert* in the inspection – similarly to search and seizure – can guarantee professionalism, credibility and unchangingness of the evidence. In the proceedings where electronic data are concerned, the involvement of an IT expert could be important if the inspection of the information system or data medium requires special knowledge, while in order to collect electronic evidence a *specialist consultant* can be used.[6] The specialist consultant is not an expert, but is a person with expertise on a specific issue not specifically defined by law. He assists the authorities by providing expertise where specific knowledge is required to detect, search for, acquire, collect or record evidence. He provides information of a specific nature to supplement the expertise of the authorities. A specialist consultant may be interrogated as a witness regarding a procedural act carried out with his involvement (HCCP 270. § (1) and (5) and the justification for the given article of the Act).

Evidence found on the internet is usually saved as part of the online inspection. In data saving, the acting investigators search and record relevant data such as internet searches and downloaded files.[7]

On-site interrogation, reconstruction of a criminal offence, presentation for identification and confrontation have little if any significance in cybercrime cases, so we will only briefly describe their essence.

8.3.2.2. *On-Site Interrogation*

On-site interrogation gives the court, the prosecution service, or the investigating authority an opportunity to interrogate the defendant and the witness on the site. This is done if it is necessary

[6] See B. Simon, R. Gyaraki, *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020, p. 138.
[7] Ibidem.

that they give testimony at the scene of the criminal offence or at another place related to the criminal offence or to show the place where the criminal offence was committed, another place related to the criminal offence, to show physical evidence or the course of the criminal offence (HCCP 208. § (1) para.).

8.3.2.3. *Reconstruction of a Criminal Offence*

Reconstruction of a criminal offence may be ordered and held by the court, the prosecution service or the investigating authority if it is necessary to establish or verify whether an event or phenomenon could have occurred at a specific place, time, in a specific manner or under specific circumstances. It shall, as far as it possible, be held under the same conditions as the event or phenomenon under investigation occurred or could have occurred (HCCP 209. § (1) para.).

8.3.2.4. *Presentation for Identification*

Presentation for identification can be ordered and held by the court, the prosecution service or the investigating authority if doing so is necessary for the identification of a person or object. A least three persons or objects must be presented to the defendant or the witness for identification. This usually means the physical presentation of a person or an object, but in the case when no other option is available, they can be presented by visual or audio or audio-visual recording (HCCP 210. § (1) para.).

8.3.2.5. *Confrontation*

Confrontation may be necessary when the testimony of the defendants, witnesses or the defendant and the witness contradict each other. In such a case the court, the prosecution service and the investigating authority can order a confrontation in order to resolve the contradiction (HCCP 211. § (1) para.).

8.3.3. OBTAINING THE EVIDENCE

Authorities acting in criminal cases can use open and covert means to obtain the evidence necessary to establish the facts of a case. It is not possible to outline in a few sentences all that is important to know about the use of covert means in criminal proceedings in Hungary, so we only try to provide a brief overview of the most important features of these instruments.

The use of *covert means* raises several constitutional problems, because fundamental rights of citizens – even those of outsiders, who have no connection with the offence subject of the investigation – might be violated. Therefore, it is of utmost importance that the use of covert methods should be permitted only in exceptional cases, in accordance with the principles of *necessity* and *proportionality*. In order to meet these requirements, the HCCP allows the use of covert means if:

a) it can be reasonably assumed that the information or evidence to be obtained is essential for achieving the purpose of a criminal proceeding, and it cannot be obtained by other means,
b) its use does not result in a disproportionate restriction of the fundamental right of the person concerned, or of another person in relation to the attainment of the law enforcement goal and
c) it is likely that information or evidence relating to a criminal offence may be obtained by its use (HCCP 214. (5) para.).

The HCCP allows the use of several covert means in criminal proceedings.[8] It classifies covert means into *three categories* according to the permission (authorisation) they are subject to. These categories are the following:

a) not subject to permission of a judge or a prosecutor,
b) subject to permission of a prosecutor, or
c) subject to permission of a judge (HCCP 214. § (4) para.).

[8] In Poland "secret or remote searches are not allowed on the grounds of criminal procedure". P. Lewulis, *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, p. 47, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

The first group includes for example the use of a trap or covert surveillance. The surveillance of payment transactions, simulated purchases, use of an undercover investigator and some other means are allowed only with *permission of the public prosecutor*, but covert means representing the most serious restriction of fundamental right may only be used with the permission of judicial authority.

According to the HCCP the following covert means may be used only *with judicial permission*: secret surveillance of an information system, secret search, secret surveillance of a locality, secret interception of a consignment, interception of communications.

The last group of covert means play a most important role in cybercrime cases, as they might be decisive for identifying the perpetrator or to obtain access to information necessary to detect the offence. The court decides on granting permission to use any covert means subject to permission of a judge upon a motion submitted by the prosecution service. Since covert means may only be used during the investigation (or to the limited extent in the preparatory procedure) the tasks of a court of first instance are performed by a district court judge appointed as *investigating judge* by the president of the respective regional court. We intend to describe covert means typically appropriate to use in cybercrime cases in the next subchapter.

8.4. Particulars of Evidence Used in Cybercrime Cases

What is special about the evidence process in cybercrime cases? First of all, the main difficulty is how to prove the commission of such offences, to detect the identity and location of the perpetrator. Regarding crimes committed in the cyber environment, the preponderance of evidence is based on *digital data*. "The evidence of cybercrime offences exists nearly exclusively in electronic form.[9]" Many authors emphasise, that is more difficult to collect evidence and establish facts in cybercrime cases than in other cases.[10] While that may be true, it should be added that this statement is justified not

[9] J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[10] For example, I. Lajtár, *A kiberbűnözésről,* "Ügyészek Lapja" 2019, No. 1, p. 50.

only in cybercrime cases, but in other procedures where electronic data must be used as a means of evidence. Electronic data can be changed and deleted quickly and thus evidence can be destroyed or falsified. Determining the *place* where the digital data was created or/and uploaded sometimes means insurmountable tasks for law enforcement agencies. The IT service providers often lack the will to cooperate, but without their help, collection of evidence is a difficult or impossible task.

Similarly, *pinpointing the user's identity* can be extremely difficult, taking into account that the same system is frequently used by several people.[11]

Another challenge of digital investigation is *encryption*. Several forms of encryption are described by Kökényesi-Bartos, who summarises the consequence of encrypted communication as follows:

> It is not easy to observe such communication on the internet, not even by the authorities, even if the user's Internet service provider or messaging service company providing the messaging service was approached by law enforcement to provide legal assistance.[12]

Encryption is no longer a magic thing, cybercriminals have easy access to encryption solutions and software, "(…) they are available in online commerce together with software designed to remove digital evidence".[13] At the same time, unblocking the increasingly widespread and sophisticated encryption technology is also a serious challenge.[14]

---

[11] See: Ibidem.

[12] A. Kökényesi-Bartos, *The functioning of internet communication and the challenges of online digital investigation*, [in:] G. Virág (ed.), *Combating cybercrime, corruption and money laundering*, "Studies on Criminology" 2022, Vol. 59, Special Issue 2, p. 90. In his study, the author writes about solutions that hide the user's IP address, thus making it impossible to identify the user.

[13] B. Grund, *A kibertér bűncselekményeiről* és *a kiberbűnözés hazai gyakorlatáról,* p. 5, https://jog.tk.mta.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol (accessed on: 18.07.2023).

[14] I. Lajtár, *A kiberbűnözésről*, *op. cit*., p. 50.

8.4.1. ELECTRONIC DATA AS A MEANS OF EVIDENCE

As Zoltán Nagy wrote, "the range of crime that cannot be committed by computer is getting narrower".[15] Criminals use tech services and tools to plan and commit crimes more frequently. "As a result, e-evidence is becoming essential to fighting crime: currently, 85% of criminal investigations involve digital data."[16] We agree with Lewulis, who states that "The importance of digital evidence extends to the prosecution of all types of crimes in all jurisdictions."[17]

What is e-evidence? Electronic evidence, or "e-evidence", refers to *digital data* that is used to investigate and prosecute criminal offences. As Tibor Peszleg states, digital evidence is data, so it is not a tangible thing. Data does not exist in itself, it is only recorded by some data medium.[18]

Among electronic data, a distinction can be made between electronic data carrying content, traffic data or other electronic data and traces.[19] Such data can be used to identify a person or obtain more information about their activities. Electronic data includes, among others: emails, text messages or content from messaging apps, audiovisual content information about a user's online account, etc.

---

[15] Z. Nagy, *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in]: *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, "Acta Universitatis Szegediensis, Acta Juridica et Politica" 2018, Vol. 81, p. 755.

[16] European Council, *Better access to e-evidence to fight crime,* https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

[17] P. Lewulis, *Collecting…*, *op. cit.*, p. 39.

[18] T. Peszleg, *A digitális bizonyítási eszközök megszerzésének elvei* és *gyakorlati érvényesülésük,* "Ügyészek Lapja" 2010, No. 2, p. 26.

[19] See more about the classification in: Z. Nagy, *A joghatóság…*, *op. cit.*, p. 758. Claudia Warken states, that "The common distinction of communication data, generally resulting in a classification of content data and non-content data or content data, traffic data and user data, does not meet the requirements of modern legistics. (…) The required classification has to reflect the sensitivity of specific types of electronic data." In her study she provides a comprehensive data classification for criminal law purposes. C. Warken, *Classification of Electronic Data for Criminal Law Purposes*, "Eucrim" 2018, No. 4, p. 226.

When using the internet, the user leaves traces, which in the event of committing a criminal offence can help identify the perpetrator and clarify circumstances of the offence.[20] If the subscriber is the same as the user, the investigating authorities has an easier task. However, if the given subscription is used more than one person, identifying the alleged perpetrator is much more difficult, and the fact that a subscriber's IP address is not permanent also causes problem. In the case of dynamic IP address allocation based on the given IP address alone, it is not possible to determine which internet subscriber used it, only if we know the exact time of use. The service provider logs which IP address was used by which customer at which time and can provide this information at the request of the authorities.

Electronic data, like other data required in criminal proceedings, can be obtained by both open and covert means. The provision on *open data acquisition* is set out in 261. § of the HCCP under the heading of data collection activities. Authorities acting in the criminal procedure may request any organ, legal person, or other organisation without a legal personality to provide data (HCCP 261. § (1) para.). Point b) of that section also refers specifically to electronic data. Within the framework of data request – among others – the transfer of electronic data may be requested (HCCP 261. § (3) para. b) point). The organisation requested to provide data is obliged to comply with the request within a set time limit or to notify of a detected obstacle to fulfilment without delay (HCCP 264. § (1) para.).

A special possibility of data request is conditional data request (HCCP 266. §). This means that the party obliged to provide the information must do so if and when the condition specified occurs. It means a kind of monitoring activity, allowing the monitoring of the subject concerned for a longer period of time.

"Electronic evidence of such crimes may be difficult to collect, owing to the volatility of data, and may require specific expertise."[21]

[20] See A. Kökényesi-Bartos, *The functioning…*, *op. cit*., p. 86.

[21] *Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime November 2020*, p. 3, https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf (accessed on: 11.07.2023).

In the process of obtaining and collecting electronic data, particular care must be taken to ensure that their authenticity cannot be questioned, otherwise their use before the court will fail and they will not be accepted as evidence by the court.[22] The success of proving crimes committed in the IT environment is decisively influenced by the fact whether the investigating authority or the public prosecutor can ensure electronic data proving the commission of the crime during the investigation.[23]

From the point of view of collecting and recording electronic data, it is also important where they are located. Whether we are talking about data stored on a physical device (computer, phone etc.) or in the cloud.[24]

The Polish Code of Criminal Procedure:

> formally recognizes only two general types of evidence sources: personal and material (or real) evidence. (…) Since digital information does not possess a physical form, digital evidence placement in such an exhaustive division of evidence types might be problematic. However, out of necessity digital evidence falls into the "material evidence" category despite not having a physical form.[25]

But in Poland, 'there is no legal definition of "digital evidence"'.[26]

In criminal proceedings – not only concerning cybercrime cases but all cases where electronic data should be used as evidence – the access to electronic data stored in another country is crucial. In the EU, the adoption of new rules to speed up access to electronic/digital data started in 2018[27] when the European Commission put

[22] This is often emphasised by authors who write about collecting evidence. See for example: B. Simon, R. Gyaraki, *op. cit*., pp. 132, 135.

[23] I. Szabó, *Az elektronikus bizonyítékok megszerzésének időszerű problémái*, "Ügyészségi Szemle" 2018, No. 3, p. 116.

[24] See: B. Simon, R. Gyaraki, *A kiberbűncselekmények…*, *op. cit.,* p. 126.

[25] P. Lewulis, *Collecting…*, *op. cit*., p. 42.

[26] Ibidem.

[27] But the start of the process goes back to 2016, when "the Council called for concrete action based on a common EU approach to make mutual legal

forward a proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.[28] What do the Production Order and Preservation Order mean?

> The production order will allow a member state's judicial authority to directly request access to e-evidence from a service provider established or represented in another member state (…) The preservation order will prevent e-evidence from being deleted by a service provider while the production order is still being processed.[29]

From this very short introduction, it is obvious that the new regulation makes access to electronic data much easier and faster, and consequently makes the investigation and prosecution more effective.[30]

---

assistance more efficient; to improve cooperation between Member State authorities and service providers based in non-EU countries; and to propose solutions to the problem of determining and enforcing jurisdiction in cyberspace." Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Strasbourg, 17.4.2018. COM (2018) 225 final, (hereinafter: Proposal for Production and Preservation Order), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed on: 26.07.2023). The concrete background of the proposal was the terrorist attacks in Brussels of 22 March 2016 and the Joint Declaration of EU Ministers for Justice and Home Affair Ministers and Representatives of EU Institutions' two days after the attacks. See: Á.Tinoco-Pastrana, *The Proposal on Electronic Evidence in the European Union*, "Eucrim" 2020, No. 1, p. 46.

[28] Proposal for Production and Preservation Order.

[29] European Council, *Better access to e-evidence to fight crime*, https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

[30] On 25 January 2023 the EU member states' ambassadors "confirmed the agreement reached between the Council presidency and the European Parliament on the draft regulation and the draft directive on cross-border access to e-evidence," https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-

8.4.2. IT EXPERT IN CRIMINAL PROCEEDINGS

In cybercrime cases, certain *special knowledge* may be necessary to determine what kind of evidence should be collected and which coercive measure if any should be used in order to collect it. Since the possibility of using electronic evidence may emerge in more and more cases, "There is a constantly increasing demand for the expertise and opinion of an IT or computer expert in criminal proceedings."[31]

Expert opinion is a very important piece of evidence. It is frequently used in cybercrime cases because members of the investigating authority, the public prosecutor and the judge do not have special technical knowledge – although they usually, but not necessarily, have user-level knowledge. "Digital traces can usually only be searched for and interpreted by people with expertise."[32]

The Hungarian CCP provides a relatively wide possibility for the involvement of the expert. If specialised expertise is required to establish or determine a fact to be proven, an expert shall be employed (HCCP 188. § (1) para.).

Regarding the involvement of the expert, it should be noted that it is neither appropriate to involve him in the procedure unnecessarily, nor to not involve him in the procedure even when necessary.[33]

---

on-new-rules-to-improve-cross-border-access-to-e-evidence/ (accessed on: 26.07.2023). The 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 and the Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings were adopted on 12 July 2023 and were published in the Official Journal of the European Union on 28 July 2023.

[31] B. Elek, *Informatikus szakértés a büntetőeljárásban*, "Belügyi Szemle" 2014, No. 7–8, p. 163.

[32] T. Peszleg, *Interneten, számítógépen történő nyomrögzítés*, "Ügyészek Lapja" 2005, No. 1, p. 27.

[33] "Currently, it can generally be said that in cyber related cases of crimes the investigating authority appoints an expert because they are either afraid that the digital evidence will not be recognized, or because they fear that a procedural mistake will be made when implementing the coercive measure" or

With respect to the former, the appointment of an expert may result in unjustified prolongation of the procedure and higher procedural cost, while in the latter case, unrecoverable errors may occur:

> The analysis of digital evidence requires appropriate IT knowledge, which is often not available to the staff of the investigating authority. The forensic IT expert is the only actor in the criminal justice proceeding who can and is entitled to help in this situation.[34]

In 2020 a *methodological letter* was adopted on general principles for the examination of electronic data.[35] The material scope of this methodological letter covers the following areas of forensic informatics expert activity related to electronic data: identification, preservation, collection, conservation, acquisition, examination, and analysis of electronic data.

Experts also play a very important role in criminal proceedings in Poland, because "Polish law does not describe any specific technics or methods of material evidence gathering, leaving that to experts in relevant disciplines of forensic science."[36]

8.4.3. COVERT METHODS USED FOR OBTAINING EVIDENCE IN CYBERCRIME CASES

It is not possible to present all covert means in the framework of this chapter, so we will only briefly mention those that may be relevant to the detection of cybercrimes.

---

the prosecutor requires the appointment of an expert. B. Simon, R. Gyaraki, *A kiberbűncselekmények…*, *op. cit*., p. 146.

[34] I.Zs. Máté, *Az igazságügyi informatikai szakértő a büntetőeljárásban – doktori értekezés,* Pécs 2017, p. 112, https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/mate-istvan-zsolt/mate-istvan-zsolt-vedes-ertekezes.pdf (accessed on: 06.08.2023).

[35] Methodological letter No. 6/2020, https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf (accessed on: 06.08.2023).

[36] P. Lewulis, *Collecting…*, *op. cit*., p. 44.

Surveillance of Payment Transactions

Surveillance of payment transactions is one of the *covert means* subject to *permission of the public prosecutor*. The essence of this measures is, that an organisation providing financial services or supplementary financial services may be instructed to record, keep, and transmit data pertaining to payment transactions to the ordering entity during a specified period (HCCP 216. § (1) para.). In addition to passive surveillance, the use of this covert means may also include the suspension of the execution of the payment transaction for the purpose of evaluating data and intervening in the interests of law enforcement (HCCP 217. § (1) para.). During the suspension of the payment transaction, the ordering entity shall examine whether the suspended payment transaction can be connected to a criminal offence (HCCP 217. § (3) para.).

Covert Means Subject to Permission of a Judge

According to the HCCP, the following covert means may be used subject to permission of a judge:

a) secret surveillance of an information system,
b) secret search,
c) secret surveillance of a locality,
d) secret interception of a consignment,
e) interception of communications (HCCP 231. §).

Although in principle all covert means subject to a judicial permission can be used in cybercrime cases as well (provided that it constitutes a criminal offence, for which the law allows the use of covert means) we highlight only one of them, the *secret surveillance of an information system*. In the course of secret surveillance of an information system, the organ authorised to use covert means may, with permission of a judge, secretly access and record, by technical means, data processed in an information system. For that purpose, any necessary electronic data may be placed in an information system, while any necessary technical device may be placed at a dwelling, other premises, fenced area, vehicle, or other object used by the person

concerned, except for public areas, premises open to the public, and means of public transport (HCCP 232. § (1) para.). Covert means subject to a judicial permission may only be used in proceedings for offences and for the time period defined by the HCCP.

8.5. *De Lege Ferenda* Proposals

Due to the difficulties in the law enforcement resulting from development of information technology, it is almost impossible to develop up-to-date laws that enable efficient justice.[37] As Hungarian researchers not being familiar enough with Polish criminal procedural law and practice, we can only very cautiously make suggestions to the legislator. As Lewulis states:

> Polish law enforcement authorities may try to bypass or even ignore the described procedural shortcomings. Given the existing legal deficiencies, it is well imaginable that digital evidence is collected with the omission, or even contrary to some regulation (…) Such evidence could be considered illegally obtained.[38]

In order to avoid such actions of law enforcement authorities which result in the inadmissibility of evidence and consequently in the ineffectiveness of prosecution, the legislator must monitor law enforcement practice and respond to problems that can be solved by legislation.

The involvement of legal practitioners in the legislative process works well in many countries. Legislators must accept that they are not infallible, and the feedback of practitioners must be taken into account in the course of the correction of legislative mistakes, especially in complex, coordinated legislative processes.

[37] I. Szabó, *Az elektronikus…*, *op. cit*., p. 116.
[38] P. Lewulis, *Collecting…*, *op. cit.,* p. 50.

It is already a commonplace that the legislator should pay attention to international expectations, which means more than just compliance with the EU's requirements.

Attention must also be paid to the proposals formulated by the scientific community.

8.6. Conclusion

Although traditional forms of evidence can also be available in cybercrime cases, they have less significance. 'The evidence of cybercrime offences exists nearly exclusively in electronic form.[39]' The importance of continuous training of legal practitioners is highlighted by several authors. It is important that the authorities in criminal matters are aware of newer methods of committing offences and of the latest trends in IT crime. To this end, Petronella Deres proposed the joint training of the members of organisations involved in criminal proceedings (investigating authorities, prosecutor's offices, courts)[40]:

> Capacity building is the most effective way towards more effective investigation, prosecution and adjudication of cybercrime and other offences involving electronic evidence. A massive surge in resources and skills for criminal justice authorities, including the judiciary is required.[41]

[39] J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[40] P. Deres, *A kibertérrel* összefüggő *bűncselekmények sajátosságai Magyarországon*, "Ügyészek Lapja" 2023, No. 1, p. 79.

[41] *Key messages of the Octopus Conference 2019. Cooperation against cybercrime, Strasbourg, 20–22 November 2019*, https://rm.coe.int/3021-110-octo19-keymessages-v3/168098e8a5 (accessed on: 10.08.2023).

REFERENCES

Belovics, E., Tóth, M., *Büntető eljárásjog*, Budapest 2017.

Deres, P., *A kibertérrel összefüggő bűncselekmények sajátosságai Magyarországon*, "Ügyészek Lapja" 2023, No. 1, pp. 75–79.

Elek, B., *Informatikus szakértés a büntetőeljárásban*, "Belügyi Szemle" 2014, No. 7–8. *Key messages of the Octopus Conference 2019. Cooperation against cybercrime 20-22 November 2019*, Strasbourg, https://rm.coe.int/3021-110-octo19-keymessages-v3/168098e8a5 (accessed on: 10.08.2023).

European Council, *Better access to e-evidence to fight crime*, https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

Farkas, Á., Róth, E., *A büntetőeljárás*, Budapest 2018.

Grund, B., *A kibertér bűncselekményeiről* és *a kiberbűnözés hazai gyakorlatáról*, https://jog.tk.mta.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol (accessed on: 18.07.2023).

Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Kökényesi-Bartos, A., *The functioning of internet communication and the challenges of online digital investigation*, [in:] Virág, G. (ed.), *Combating cybercrime, corruption and money laundering*, "Studies on Criminology" 2022, Vol. 59, Special Issue 2, pp. 82–92.

Lajtár, I., *A kiberbűnözésről*, "Ügyészek Lapja" 2019, No. 1.

Lewulis, P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, pp. 39–62, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

Máté, I.Zs., *Az igazságügyi informatikai szakértő a büntetőeljárásban – doktori értekezés,* Pécs 2017, https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/mate-istvanzsolt/mate-istvan-zsolt-vedes-ertekezes.pdf (accessed on: 06.08.2023).

Methodological letter No. 6/2020, https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf (accessed on: 06.08.2023).

Nagy, Z., *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, "Acta Universitatis Szegediensis, Acta Juridica et Politica" 2018, Vol. 81.

Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime November 2020, https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf (accessed on: 11.07.2023).

Peszleg, T., *A digitális bizonyítási eszközök megszerzésének elvei* és *gyakorlati érvényesülésük,* "Ügyészek Lapja" 2010, No. 2.

Peszleg, T., *Interneten, számítógépen történő nyomrögzítés*, "Ügyészek Lapja" 2005, No. 1.

Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM (2018) 225 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed on: 26.07.2023).

Riekkinen, J., *Evidence of cybercrime and coercive measures in Finland*, p. 1, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

Simon, B., Gyaraki, R., *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Szabó, I., *Az elektronikus bizonyítékok megszerzésének időszerű problémái*, "Ügyészségi Szemle" 2018, No. 3.

Tinoco-Pastrana, Á., *The Proposal on Electronic Evidence in the European Union*, "Eucrim" 2020, No. 1, pp. 46–50.

Warken, C., *Classification of Electronic Data for Criminal Law Purposes*, "Eucrim" 2018, No. 4.

Basic Hungarian legal sources

2016. évi XXIX. törvény az igazságügyi szakértőkről.
2017. évi XC. törvény a büntetőeljárásról.
9/2018. (VI. 29.) LÜ utasítás az előkészítő eljárással, a nyomozás felügyeletével és irányításával, valamint a befejező intézkedésekkel kapcsolatos ügyészi feladatokról.
100/2018. (VI. 8.) Korm. rendelet - a nyomozás és az előkészítő eljárás részletes szabályairól.