Questions Arising from Digital Evidence in the Hungarian Criminal Procedure

Dávid Toth*

Abstract

In combating cybercrime, it is vital that the investigative authorities be able to quickly obtain all the electronic data which can be relevant in the criminal procedure and can be presented as evidence. Many problems appeared for law enforcement in the 21st century. Questions like which country has jurisdiction to investigate for digital evidence in an international cybercrime case. How can we seize cryptocurrencies (e.g., bitcoin)? Hungary has adopted a new Criminal Procedure Code in 2017, which entered into force in 2018 on the first of July. I would like to examine the current regulation with a descriptive approach considering these challenges.

The aim of the research is to give an overview of the practical problems and the regulation of the criminal procedure in connection with digital evidence. In the last part of the article, my goal is to give proposals for the legislature on the development of the relevant legal provisions.

Keywords: *digital evidence, criminal procedure, cryptocurrencies.*

I. Introduction

Thanks to the information technology revolution of the 21st century, people are increasingly communicating with each other in the online space through smart devices, and the pandemic caused by Covid 19 has even steered the worlds of work and education more towards cyberspace[1]. In this situation, people leave more digital traces daily (so-called digital footprint).

In combating cybercrime, it is vital that the investigative authorities be able to quickly obtain all the electronic data which can be relevant in the criminal procedure and can be presented as evidence. Furthermore, we can also see that there is a growing demand for the knowledge and opinion of an IT professional in criminal proceedings[2].

The research aims to give an overview of the practical problems and the regulation of the criminal procedure in connection with digital evidence. In the last part of the

* Ph.D., Senior Lecturer, Criminology and Penal Law Department, University of Pécs, Faculty of Law, Hungary. Contact: toth.david@ajk.pte.hu.

[1] I.L. Gál, *A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre* [Potential effects of the coronavirus (COVID-19) and the global economic crisis on crime], in Magyar Jog no. 5/2020, pp. 257-265.

[2] E. Balázs, *Informatikus szakértés a büntetőeljárásban* [IT expertise in criminal proceedings], *in* Belügyi Szemle, 7-8/2014, pp. 158-180.

article, my goal is to give proposals for the legislature on the development of the relevant legal provisions.

II. Basic concepts

There are many concepts in the legal literature for proof. According to Herke, Fenyvesi, and Tremmel, proof is a cognition process, where the authorities aim to explore the events that happened in the past for a single case. In this procedure, authorities collect evidence and data which can be relevant to the criminal case in which they investigate. The result of proof is that the court can establish the statutory provisions according to the truth. The process must have a legal basis. In their concept, they aimed to combine different approaches to the proof definition[3].

Evidence in criminal proceedings is data related to criminally relevant facts which are obtained from sources permitted by law, and which may therefore be used in their entirety to determine the relevant statutory provisions of criminal law by the deciding authority[4].

For a long time, the taxonomic place of electronic data in Hungarian criminal law was not sufficiently clarified[5]. Our previous Criminal Procedure Code (the Act XIX of 1998) only contained the definition of physical evidence. Electronic data was not listed as mean of proof[6]. Under Section 115 of the previous Code, any object was considered as physical evidence if they were suitable for proving the facts to be proven. A typical example for this could be an object bearing the marks of the commission of the crime. Documents, drawings, and any data-recording objects were also included in the definition[7].

It was time to amend the regulation because people use more and more electronic telecommunication devices daily and the electronic data recorded and stored on them can be vital evidence in certain cases. The justification of the Code favored the separate naming of electronic data because these cannot be treated in all cases by analogy with physical evidence. In accordance with this, the Code defines the concept of electronic data in a chapter together with physical evidence. The law also treats electronic data as physical evidence, unless otherwise provided.

According to the law, electronic data is the appearance of facts, information, or concepts in any form which can be processed by an information system. Under the Code, a program that provides the execution of a function by the information system is also considered electronic data. Where the Code mentions a material means of proof, electronic data shall also be understood, unless otherwise provided (Section 205). This definition is similar to the Convention on Cybercrime's concept of computer data [Convention on Cybercrime from the Council of Europe (Budapest, 23.XI.2001) Article 1]. Overall, we

---

[3] C. Herke, C. Fenyvesi, F. Tremmel, *A büntetőeljárásjog elmélete* [Theory of criminal procedure law], Budapest-Pécs, Dialog Campus Kiadó, 2012, pp. 125-138.

[4] *Ibidem.*

[5] K. Sorbán, *A digitális bizonyíték a büntetőeljárásban* [Digital evidence in criminal proceedings] in Belügyi Szemle no. 11/2016, pp. 81-96.

[6] L. Dornfeld, *Az elektronikus bizonyítékszerzés aktuális kérdései* [Current Issues in Electronic Evidence] in Kriminológiai Közlemények no. 77/2017, pp. 241-256.

[7] I.Z. Máté, *A digitális bizonyíték* [Digital evidence] in IX. Jogász Doktoranduszok Országos Szakmai Találkozója [IXth National Professional Meeting of Doctoral Students in Law] 2013, Budapest, Károli Gáspár Református Egyetem, pp. 86-94.

can note that not just a single file, like a digital video, can be considered as electronic data but also an operating system in its entirety[8].

Electronic data may be generated on personal devices like smartphones or personal computers as well as high-performance servers, networks, or cloud services (e.g., iCloud, google drive etc.). Electronic data can carry different information and based on this we can differentiate between content data or metadata[9]. E-mails, chat messages, files can be examples of the former. The latter is a set of data that describes and gives information about other data. A good example for metadata can be log files on a server, or music file metadata might include the artist's name or genre of the song[10].

III. Issues on manipulating digital evidence and legality

Electronic data is often volatile and stored data can be easily and quickly manipulated, even without a trace. By breaking down a particular information system, the data stored in the system can also change. The integrity, and authenticity of the digital evidence must be ensured in the acquisition[11].

We could mention digital photos as an example that has been increasingly used as digital evidence in criminal proceedings. There are concerns about these photos whether can be admissible in front of a court hearing because these photos can be manipulated with computer software (e.g., Photoshop)12. There are also many smartphone applications nowadays that can alter the original photos.

Other concerns are related to online text messages and comments. There can be cases where somebody is framed or staged to commit a crime while they have nothing to do with these messages. Personal accounts can be hacked, and this can lead to the so-called criminal identity theft phenomenon and in unfortunate cases can result in *Justizmord* where innocent people are found guilty[13].

Digital traces can usually only be found and interpreted by qualified people. Very often, not only special expertise but also special tools are needed to retrieve this information. Obviously, in these cases, IT experts must take part and analyze digital evidence according to the law. However, at the end, the judge shall decide on the digital evidence whether will be admissible or not[14]. The judge shall ask the right questions

---

[8] I. Szabó, *Az elektronikus bizonyítékok megszerzésének időszerű problémái* [Timely problems in obtaining electronic evidence] in Ügyészségi Szemle no. 3/2018, pp. 117-160.

[9] A. Kraut, L. Kőhalmi, D. Tóth, *Digital Dangers of Smartphones,* in Journal of Eastern-European Criminal Law no. 1/2020, pp. 36-49.

[10] T. Ibolya, *XXXIII. Fejezet. Tárgyi bizonyítási eszköz, elektronikus adat* [XXXIIIth Chapter. Material means of proof, electronic data] in Kommentár a büntetőeljárási törvényhez [Commentary on the Code of Criminal Procedure], Budapest, Wolters Kluwer, pp. 459-460.

[11] *Ibidem*.

[12] D.P. Nagosky, *The admissibility of digital photographs in criminal cases,* FBI L. Enforcement Bull., 2005, p. 1.

[13] D. Tóth, *Az identitáslopás kriminológiai sajátosságai* [Criminological features of identity theft] in A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői [Law Enforcement Factors in Law Enforcement and Crime Prevention], Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2019, pp. 207-213.

[14] A. Bendes, *A szakértő szerepe a digitális adat elemzése során a büntetőeljárásban* [The role of the expert in the analysis of digital data in criminal proceedings] in I-II. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai [I-II. Conference volume: Presentations of the conference organized for doctoral students of law in Pécs], Pécsi Tudományegyetem Állam– és Jogtudományi Kar Doktori Iskola, Pécs, 2021, pp. 68-76.

to the expert and interpret the expert's opinion. This is a somewhat paradoxical situation where the expert understands the major facts on the evidence and the court will just filter the essence of it (the so-called iceberg effect). Parti recommends that lawyers should be trained in basic IT skills. Lawyers equipped with IT skills will see not only the surface of the case, but they will already have ideas about what might have happened to the digital evidence and what aspects should be examined[15].

In connection with this, the evidence must be traced, gathered, secured, and used in compliance with the provisions of the in-force regulation irrespective of the physical or digital nature. In this aspect, two parties have duties to ensure legality. On one hand the lawmaker more precisely, the Parliament must lay down and set the rules for the proof system. The lawmaker must follow the changes in society and give a legal framework for the new life situations.

On the other hand, law enforcement must apply and follow the legal framework to ensure that justice is delivered in individual cases. They shall collect evidence pursuant to the law and eliminate the possibility of using tampered, misleading, or irrelevant evidence. During the evaluation of the evidence, the authorities shall apply the law as well.

This also imposes an obligation on law enforcement to refrain from certain acts. Facts derived from means of evidence obtained by the court, the prosecution office, or the investigating authority by way of committing a criminal action, by other illicit methods, or by the substantial restriction of the procedural rights of the participants may not be admitted as evidence in the criminal procedure. These general rules for legality must be supplemented with special provisions for the seizure and use of digital evidence.

IV. Coercive measures in connection with digital evidence

4.1. The seizure of electronic data

There are several coercive measures in the Criminal Procedure Code in relation to electronic data. Digital evidence may be seized. There is also the possibility for an obligation to preserve it or render it inaccessible temporarily.

Seizure as a coercive measure restricts the ownership of electronic data. The purpose of seizure is to obtain and preserve digital evidence for the criminal procedure[16]. The seized electronic data may contribute to the final verdict on innocence or guilt. The first question that arises is what exactly should be seized? There are three options in practice:

- seizure of the whole information system (e.g., the entire computer);
- seizure of the storage device that contains the relevant data (e.g., hard drive, or Solid-State Drive); or
- seizing only, the electronic data itself.

The first option can infringe fundamental privacy rights as many irrelevant parts of the computer will be seized which might rapidly be depreciated due to the development of technology, so it might cause financial damage as well[17].

---

[15] K. Parti, *Újratervezés, avagy miért fontos az elektronikus bizonyítékszerzés?* [Redesign, or why is electronic taking of evidence important?] in Rendészeti Szemle no. 3/2010, p. 101.

[16] M. Tóth, *A bizonyítás a büntetőeljárásban* [Evidence in criminal proceedings] in Büntető eljárásjog, Budapest: Hvg-orac Könyvkiadó, 2020, pp. 156-195.

[17] K. Sorbán, cited, pp. 81-96.

In some cases, not a single computer, but a whole server of a company might be seized which can also cause a significant financial damage to the company. The second possibility has the advantage of causing less damage to the person who suffers the seizure but on the other hand, always requires an expert for the procedure[18]. The first option used to be the practice for many years. Even the monitor or the keyboard or mouse were taken away by the police.

According to Peszleg's view, it is not enough for the investigating authority to remove only the data carriers from the computer for fear of seizing devices that are redundant during the proceedings. He mentions examples of Redundant Array of Inexpensive Disks (RAID) arrays. If the device unit is disassembled, it is no longer possible to restore the original data contained in this case[19].

According to the in-force Criminal Procedure Code, the seizure of electronic data can be carried out in all three ways. This means according to Section 315 (1) that:

- by making a copy
- by transferring,
- by making a copy of the entire contents of the information system or data carrier containing it,
- by seizing the information system or medium containing it.

A big novelty in the new Code is that according to Section 315 (2) the seizure of the electronic data used for payment may also be carried out by inhibiting the data subject from disposing of the value. These rules must be applied for the seizure of a document existing as electronic data.

The Code consists of the principle of necessity by laying down that the seizure of electronic data – if possible – shall be carried out only on data that are relevant to the criminal procedure. If they seize irrelevant data, the seizure of these should terminate as soon as possible.

An information system or data carrier containing electronic data may be seized if:

- it can be confiscated, or
- it is relevant as a mean of physical evidence, or
- the verification requires an examination of an unforeseeable or significant amount of electronic data stored therein.

The owner of the electronic data may request a copy of the data if this does not jeopardize the purpose of the criminal proceeding.

Ministerial decree (11/2003. (V. 8.) IM-BM-PM joint decree) as an important legal source supplements the regulation in connection with digital evidence. This decree regulates with the rules for the handling, registration, pre-sale, and destruction of seizures and criminal records and on the execution of confiscations. The decree gives frames for the technical way of executing the seizure of electronic data in Section 67. Pursuant to this, the seizure of electronic data shall be carried out by making a copy if:

- the conditions for leaving the seized object in the custody of the person concerned are met, and
- the continued storage of the data in the original place after the copy has been made does not jeopardize the interests of criminal proceedings.

In justified cases, a specialist consultant shall be used to make the seizure.

---

[18] *Ibidem*.

[19] T. Peszleg, *A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük* [Principles of the acquisition of digital means of proof and their practical application], in Ügyészek Lapja no. 2/2010, pp. 23-32.

When seizing electronic data, copying should, as far as possible, take place on a medium that cannot be subsequently altered.

If the data subject requests the sale of electronic data used for payment, this may be waived only if this is also necessary for proof.

Seized electronic data must be stored on a data carrier or in a repository provided by the authority. If the seized electronic data is stored on a separate medium, the identification number of the exhibit must be indicated on the medium.

4.2. Issues with the seizure of cryptocurrencies as digital evidence

In 2009 new type of money appeared called cryptocurrencies, like Bitcoin and Ethereum. They should not be confused with electronic money because they have very different properties. With these currencies, they use an encryption technique to regulate the generation of units of currency and verify the transfer of funds. One of the main characteristics of cryptocurrencies is that they are decentralized[20].

To illustrate the challenges of the seizure of cryptocurrencies I would like to summarize a case report written by Eszteri. The offenders have taken an amount of bitcoin of considerable value from the victim by fraud. Eszteri was an advisor in the case ordered by the court. The two accused persons have visited the victim in winter. Later they met at a parking lot of a store. The perpetrators offered 2.5 million Forints for 15 units of bitcoin. The victim brought the notebook with him to the parking lot to transfer the bitcoins. He transferred the crypto money to the address assigned by the offenders. After this, the two perpetrators tried to flee from the scene in their car but eventually, the police caught them. At first time the authorities did not mention in their report that it was a financial crime, and even though the victim asked for the seizure of the IT equipment the police failed to do so. Later the indictment contained the crime of fraud which caused a considerable amount of damage. The offenders transferred the bitcoins to several addresses, and these were untraceable. The seizure probably would have prevented the loss of the 15 units of bitcoin[21]. At the time of the case, it was a problem that the regulation did not deal with the seizure of these virtual currencies, but as I mentioned before Section 315 (2) of the new Criminal Procedure Code created the possibility of this[22].

How can we ensure the value of cryptocurrencies? To answer this question, some basic technical knowledge is required of how crypto money works. In the case of Bitcoin, you need a wallet (a program) to store your virtual coins. This wallet has a unique address that can be created by a certain algorithm (in the case of bitcoin it is called an elliptical curve digital signature algorithm). The algorithm creates a private key and a public key which are mathematically linked to each other. The public key will be the owner's address (just like a bank account number) while the private key proves who is the owner of the wallet. The private key allows the owner to spend his crypto money. A standard bitcoin wallet will create a wallet.dat file containing its private key.

In the case of bitcoin, the blocks represent a financial value that is never in the possession of the entitled person. The person only has the right to disposal. The

---

[20] B. Simon, *Kriptovaluták – rendészeti válaszok* [Cryptocurrencies – law enforcement responses] in Belügyi Szemle no. 10/2018, p. 77.

[21] D. Eszteri, *Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések* [A crime against property committed with Bitcoin and certain related legal issues], Infokommunikáció és Jog, 2017, pp. 25-31.

[22] A. Czine, *49. A lefoglalás* [49. The seizure] in Büntető eljárásjog, Budapest: Patrocinium, 2020, pp. 243-252.

authorities may seize the wallet.dat file but this might not always ensure the value. As Szathmáry points out the seizure of the wallet.dat file will be successful with guarantees if only one file exists of it. The most reassuring way to ensure the value would be to force the owner to transfer the crypto money to a (bitcoin) wallet of the authority[23]. There can be even cases where no wallet.dat file exist at all because the owner deleted them and decided to memorize (so-called brain wallet). In these situations, it would be impossible to seize the cryptocurrency without the cooperation of the owner[24]. Overall it is a very difficult task for the lawmaker to give perfect regulation as technology advances so rapidly. It is a positive change in the current Criminal Procedure Code that the seizure of cryptocurrencies became possible. Generally, it is expected from the regulation to have a framed nature and to be sufficiently flexible for upcoming challenges of the revolution of information technology.

4.3. Obligation to preserve electronic data

The international legal background of this institution was based on Article 16 (about the expedited preservation of stored computer data) of the Convention on Cybercrime which was adopted under the auspices of the Council of Europe and was signed in Budapest[25]. Act I of 2002 modified the previous Criminal Procedure Code and introduced it to the Hungarian system in 2003 first of July[26].

This coercive measure restricts the right of the person to dispose of the data in his possession. It can be considered as a special coercive measure because it is not carried out by the authority but by a non-criminal person to whom the provision is addressed.

The obligation to retain electronic data shall be imposed by a court, prosecutor's office, or investigative authority.

An obligation to retain electronic data may be imposed in order:

- to detect a means of proof,
- to provide a means of a proof; or
- to establish the identity or actual whereabouts of the suspect.

The data subject shall prevent the alteration, deletion, destruction, transmission of the electronic data, unauthorized copying of the electronic data, or unauthorized access thereto.

During the period of coercive measures, the electronic data which are subject to the retention obligation may be accessed only with the permission of the court, the prosecutor's office, or the investigating authority and the person obliged to retain the retention order.

Following the obligation to retain electronic data, the person ordering the retention obligation shall immediately begin the review of the electronic data. As a result of the review, the person ordering the retention order decides whether to order another way of carrying out the seizure or terminates the retention order. The retention obligation lasts for a maximum of three months. The obligation to retain will cease once the criminal

---

[23] Z. Szathmáry, *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban* [Provision of electronic money and bitcoin in criminal proceedings], in Magyar Jog no. 11/2015, 62, pp. 639-647.

[24] V. Halász, *A bitcoin működése és lefoglalása a büntetőeljárásban* [Operation and seizure of bitcoin in criminal proceedings] in Belügyi Szemle no. 7-8/2018, pp. 117-146.

[25] L. Dornfeld, *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések* [Coercive measures in connection with cybercrime], Belügyi Szemle no. 2/2018, pp. 115-135.

[26] T. Ibolya, cited, p. 459.

proceedings have been completed. The detainee shall be informed of the termination of the criminal proceedings. [Section 316 (1)-(10) of the Criminal Procedure Code]

4.4. Making the electronic data temporarily inaccessible

This coercive measure was introduced in the criminal procedure in 2013 first of July just like the new Criminal Code of Hungary (Act C of 2012). The Criminal Code created a new measure called irreversibly rendering electronic information inaccessible.

The goal of the coercive measure called making the electronic data temporarily inaccessible is to ensure the enforceability of the criminal law measure and to limit the continuation of the infringements intended to be repaired in this way until the end of the criminal proceedings.

This coercive measure can be applied if two conditions are met:

- First, the temporary unavailability of electronic data may be ordered if the criminal procedure began due to public prosecution.
- Second condition is that it is necessary to make electronic data on the offense permanently inaccessible (e.g., child pornography) to interrupt the criminal offense. This coercive measure shall be ordered only by the court.

Temporary inaccessibility of electronic data may be ordered:

- by temporarily removing the electronic data, or
- by temporarily blocking access to electronic data.

The temporary removal of electronic data and the obligation to retain electronic data may be ordered together. The Criminal Procedure Code also gives the possibility of temporary removal of electronic data and temporary blocking of access to electronic data. The latter can be used in cases related to certain crimes like drug trafficking, child pornography, the act of terrorism, terrorism financing etc.[27].

The court shall by its decision oblige the electronic communications service providers to temporarily block access to the electronic data. In this coercive measure, the National Media and Infocommunications Authority (in Hungarian Nemzeti Média- és Hírközlési Hatóság abbreviated as NMHH) have a role as well which is a central state administration body in Hungary. The NMHH performs the tasks of regulating and supervising the communications and media sector in Hungary. The court shall immediately notify the NMHH about the application of the measure. After this, the NMHH shall organize and control the implementation of the coercive measure.

Lastly, the Code regulates the call for voluntary removal of electronic data, If the interests of criminal proceedings are not harmed, the prosecutor's office or the investigating authority may call on the media content provider pursuant to the Act on Freedom of the Press and Basic Rules of Media Content to order the electronic data to be removed voluntarily. The request is optional and aims to speed up the blocking of access to electronic data. (Section 338).

V. Jurisdictional challenges

Due to character limitations, I would like to just briefly mention the jurisdictional challenges of digital evidence. Jurisdiction is a legal term used in international law. Under this institution, a state has the right to legislate, apply and enforce the law. The

[27] L. Kőhalmi, *Gondolatok a vallási indíttatású terrorizmus ürügyén* [Thoughts on the pretext of religiously motivated terrorism], in Belügyi Szemle 7-8/2015, pp. 52-71.

jurisdiction creates the possibility of the application of the law. Due to the internet digital evidence can be found in different countries in certain legal cases. Cyber-attacks can be initiated from one country and the victim can be found in another country. In the end, this can lead to jurisdictional conflicts when more states have the right and the intention to proceed in a criminal case containing international elements (so-called positive jurisdictional collision). We elaborated on this issue in another article with my colleague in detail[28]. The European Union created in 2018 a package of the proposal which could solve these issues in the future[29]. The new system would make the procedure faster for judicial authorities to access data of criminal investigations[30]. Unfortunately, these have not been adopted yet until the study was written.

VI. Summary and suggestions

In my opinion, it will be necessary for the future to train lawyers (especially judges, prosecutors, attorneys) with the basic information about the challenges of digitalization. We should also consider creating special branches within courts that deal with cases where cybercrime and digital evidence are determinative.

Mezei argues that the regulation is a step forward, but the methodological issues of seizure should be addressed by the law[31]. In my opinion, the current legislation on a statutory level is sufficient and meets the criteria to be precise clear, and necessary[32]. The methodological issues might be regulated in more detail on a decree level. On the other hand, the substantive criminal law still has not dealt with cryptocurrencies which are currently in a legally grey area in this aspect. These payment methods are not considered as money or cash-substitute payment instruments which should be changed in the future in order to have a comprehensive regulation.

References

1. Balázs, E., *Informatikus szakértés a büntetőeljárásban* [IT expertise in criminal proceedings], *in* Belügyi Szemle, 7-8/2014.

2. Bendes, A., *A szakértő szerepe a digitális adat elemzése során a büntetőeljárásban* [The role of the expert in the analysis of digital data in criminal proceedings] in I-II. Konferenciakötet: A pécsi jogász doktoranduszoknak szervezett konferencia előadásai [I-II. Conference volume: Presentations of the conference organized for doctoral students of law in Pécs], Pécsi Tudományegyetem Állam – és Jogtudományi Kar Doktori Iskola, Pécs, 2021.

[28] D. Tóth, Z. Gáspár, *Jurisdictional challenges of cybercrime,* in Journal of Eastern-European Criminal Law no. 2/2020, pp. 101-118.

[29] L. Dornfeld, *A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban* [Regulation of cross-border electronic taking of evidence in the EU], in Infokummikáció és Jog 73, 16, 2020, pp. 37-42.

[30] A.T. Pastrana, *The proposal on electronic evidence in the European Union*, in Eucrim: The European Criminal Law Associations' Forum, 2020, pp. 46-50.

[31] K. Mezei, *Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok* [Challenges and regulatory innovations in electronic evidence] in Belügyi Szemle no. 10/2019, pp. 25-40.

[32] L. Kőhalmi, *A büntetőjog alapproblémái* [Basic problems of criminal law], Pécsi Tudományegyetem Állam – és Jogtudományi Kar, Pécs, 2012.

3. Czine, A., *49. A lefoglalás* [49. The seizure] in Büntető eljárásjog, Budapest: Patrocinium, 2020.

4. Dornfeld, L., *A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban* [Regulation of cross-border electronic taking of evidence in the EU], in Infokummikáció és Jog 73, 16, 2020.

5. Dornfeld, L., *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések* [Coercive measures in connection with cybercrime], Belügyi Szemle no. 2/2018.

6. Dornfeld, L., *Az elektronikus bizonyítékszerzés aktuális kérdései* [Current Issues in Electronic Evidence] in Kriminológiai Közlemények no. 77/2017.

7. Eszteri, D., *Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések* [A crime against property committed with Bitcoin and certain related legal issues], Infokommunikáció és Jog, 2017.

8. Gál, I.L., *A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre* [Potential effects of the coronavirus (COVID-19) and the global economic crisis on crime], in Magyar Jog no. 5/2020.

9. Halász, V., *A bitcoin működése és lefoglalása a büntetőeljárásban* [Operation and seizure of bitcoin in criminal proceedings] in Belügyi Szemle no. 7-8/2018.

10. Herke, C., Fenyvesi, C., Tremmel, F., *A büntetőeljárásjog elmélete* [Theory of criminal procedure law], Budapest-Pécs, Dialog Campus Kiadó, 2012.

11. Ibolya, T., *XXXIII. Fejezet. Tárgyi bizonyítási eszköz, elektronikus adat* [XXXIIIth Chapter. Material means of proof, electronic data] in Kommentár a büntetőeljárási törvényhez (Commentary on the Code of Criminal Procedure), Budapest, Wolters Kluwer.

12. Kőhalmi, L., *A büntetőjog alapproblémái* [Basic problems of criminal law], Pécsi Tudományegyetem Állam – és Jogtudományi Kar, Pécs 2012.

13. Kőhalmi, L., *Gondolatok a vallási indíttatású terrorizmus ürügyén* [Thoughts on the pretext of religiously motivated terrorism], in Belügyi Szemle no. 7-8/2015.

14. Kraut, A., Kőhalmi, L., Tóth, D., *Digital Dangers of Smartphones,* in Journal of Eastern-European Criminal Law no. 1/2020.

15. Máté, I.Z., *A digitális bizonyíték* [Digital evidence] in IX. Jogász Doktoranduszok Országos Szakmai Találkozója [IXth National Professional Meeting of Doctoral Students in Law] 2013, Budapest, Károli Gáspár Református Egyetem.

16. Mezei, K., *Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok* [Challenges and regulatory innovations in electronic evidence] in Belügyi Szemle no. 10/2019.

17. Nagosky, D. P., *The admissibility of digital photographs in criminal cases,* FBI L. Enforcement Bull., 2005.

18. Parti, K., *Újratervezés, avagy miért fontos az elektronikus bizonyítékszerzés?* [Redesign, or why is electronic taking of evidence important?] in Rendészeti Szemle no. 3/2010.

19. Pastrana, A.T., *The proposal on electronic evidence in the European Union*, in Eucrim: The European Criminal Law Associations' Forum, 2020.

20. Peszleg, T., *A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük* [Principles of the acquisition of digital means of proof and their practical application], in Ügyészek Lapja no. 2/2010.

21. Simon, B., *Kriptovaluták – rendészeti válaszok* [Cryptocurrencies – law enforcement responses] in Belügyi Szemle no. 10/2018.

22. Sorbán, K., *A digitális bizonyíték a büntetőeljárásban* [Digital evidence in criminal proceedings] in Belügyi Szemle no. 11/2016.

23. Szabó, I., *Az elektronikus bizonyítékok megszerzésének időszerű problémái* [Timely problems in obtaining electronic evidence] in Ügyészségi Szemle no. 3/2018.

24. Szathmáry, Z., *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban* [Provision of electronic money and bitcoin in criminal proceedings], in Magyar Jog no. 11/2015, 62.

25. Tóth, D., *Az identitáslopás kriminológiai sajátosságai* [Criminological features of identity theft] in A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői [Law Enforcement Factors in Law Enforcement and Crime Prevention], Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2019.

26. Tóth, D., Gáspár, Z., *Jurisdictional challenges of cybercrime* in Journal of Eastern-European Criminal Law no.2/2020.

27. Tóth, M., *A bizonyítás a büntetőeljárásban* [Evidence in criminal proceedings] in Büntető eljárásjog, Budapest: Hvg-orac Könyvkiadó, 2020.