András Péter Bodnár[1]

Digitization in criminal proceedings – issues related to eletronic data

„New technology is not good or evil and of itself. It's all about how people choose use it."
(David Wong)

Introduction[2]

The quote outlined above largely predicts which topic, which segment of it will be examined in the following. The aim of this dissertation is to process a small slice of a topic, to answer some of the many uncertain questions waiting to be answered, which revolve around digitization, the emergence of technology in law.

We are not making an ill-considered statement by saying that technology has been penetrating our daily lives for years, decades, but at an ever-accelerating pace, mostly with the aim of making our lives more comfortable and easier. However, this development also has a number of disadvantages.

Narrowing down the discussion of the topic to my field of research, criminal procedure, I want to focus on this area of law in the future. Of course, digitalisation and technological development are also having an impact in this area, be it positive or negative. The derogations of the IT explosion that can be felt from the point of view of criminal proceedings are mostly embodied in various crimes that are somewhat related to informatics and cyberspace, but not specifically related to cybercrime.[3] As a result of the explosion of information technology and telecommunications, both parties – the private perpetrator and the investigating authority – have acquired more and more advanced technical equipment. Digitization, embodied in all segments of life, the use of the World Wide Web makes it easier to commit on the one hand and difficult to detect on the other.[4] Of course, the development of this is not due to the overnight, but to a longer arc of development. But at the same time, he has now reached a level where he is increasingly urging a response to this. Cybercrime and the crime facilitated by information technology and digitalisation have advanced into a global problem that needs to be addressed not only at the legislative and law enforcement level in each country, but also at the supranational – European Union – level.[5]

In this respect, the necessary steps have been taken on the part of the legislator, as the Criminal Code in line with EU obligations, a new measure of a security nature, even applicable on its own, has been introduced to make electronic data permanently inaccessible.[6]

The Criminal Code already explicitly mentions electronic data in connection with this measure, while the old Criminal Procedure Act (1998) in connection with the taking of evidence, he understood the electronic data as a means of physical evidence.[7]

In this respect, July 1, 2018, marked (also) a major change and milestone, when the new Criminal Procedure entered into force. The Act which raised the electronic data to an independent evidence in relation to the evidence.

Among my first questions, the following question arose in me: we can really welcome a new type of evidence to the new Criminal Procedure Act as a dowry? It has been explained above that in the previous Procedural Law Act, electronic data could be

[1] PhD student, Géza Marton Doctoral School of Legal Studies.

[2] A tanulmány megírása az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg. In the framework of the Ministry of Justice's programs to improve the quality of legal training.

[3] As an example, in 2018, about 978 million people were affected by cybercrime, in roughly 20 countries, and the number of people involved in cybercrime continues woman. Victims lost $ 172 billion worldwide, says Norton Kevin Haley From his Cyber Security Insights Report (https://www.nortonlifelock.com/about/newsroom/press-kits/ncsir-2017) (Downloaded: 2020. 10. 27.).

[4] Mráz Zoltán: *A digitális bizonyítási eszközök jelentősége a vagyon elleni bűncselekmények nyomozásában.* In.: Belügyi Szemle, 2018/7-8. 99.

[5] Gyaraki Réka Eszter: *A számítógépes bűnözés nyomozásának problémái (PhD értekezés).* Pécs, 2018. 8.

[6] Görgényi Ilona – Gula József –Horváth Tibor –Jacsó Judit – Lévay Miklós – Sántha Ferenc –Váradi Erika: *Magyar büntetőjog. Általános rész.* Wolters Kluwer Hungary, Budapest, 2019. 471.

[7] Section 115. of the old Criminal Procedure Act (1998): "For the purposes of this Act, the material means of proof shall be the document, the drawing and any object which records data by technical, chemical or other means. Where this law shall also be understood as meaning the subject of the record."

considered as a – special – type of material means of proof. If so, the question arises as to why it was necessary to regulate it as a stand-alone means of proof. Although it uses the new Criminal Procedure Act as an independent means of proof, which in its characteristics is closest to the material means of proof. This is indicated by our current procedural law itself, because Section 205. mentioned that „Where this Act mentions a material means of proof, electronic data shall be understood, unless otherwise provided in this Act."[8] In the textbook of Zsanett Fantoly and Árpád Budaházi, the reader may come across a reason for independent regulation, according to which self-regulation was necessary because electronic data cannot always be applied to the analogy of physical things in the regulation of certain criminal proceedings.[9]

1. Digitization in criminal proceedings – investigation

I explained earlier that technical progress has also made life easier for those living on the shady side of life, as it has made it much more comfortable to commit all crimes, not just those closely related to IT.

An example is the investigation of the crime of theft by violence against something committed during a travel crime. The concept of travel crime has long been part of forensics. A traveling criminal is a person who knowingly commits a crime away from his or her place of residence. In addition to the division of powers between the authorities, the perpetrator intends to take advantage of the uncertainty before the local authorities and the difficulty of recognizing the link between the crimes committed.[10] In the case of such offenses, the investigative authority's ability to detect is limited by the fact that local data collections provide little data on offenders. The widest possible use of passenger cars, the development of motorways and the enlargement of the European Union's Schengen borders have opened up new opportunities for offenders to commit more and more crimes that require more or less organization. All this without leaving their identities almost unidentifiable to the local investigating authorities.[11]

Thus, of course, it is not surprising that in recent years, among the perpetrators of burglary, in addition to Hungarian citizens, in addition to citizens of neighboring states, there have also been, for example, persons of Czech and Polish citizenship. The means of communication is the so-called work phone. The work phone is only a mobile phone that is active at the time of the crime and is used to communicate between the perpetrators. In addition to traditional telecommunications, the communication channel is, for example, the Viber application. The perpetrators use a web browser (Google Maps) to map the buildings and navigation applications to approach them.[12] This assistance with digitization has posed challenges to the perpetrators of the investigating authority. A growing percentage of facts and data relevant to reconnaissance exist on a digital basis. This process has significantly influenced the forensic activities of criminal agencies, necessitating a change in previously used procedures and mindsets. The use of an IT expert has become justified during the inspection, and the investigating authority must have the means to store and process digital traces, and the members of the investigating authority must be familiar with the concepts that can be basically associated with information technology.[13]

Remaining as an example of the crime against the said property, the digital means and traces detected during the data collection activity used in the investigation of burglary are: digitally recorded audio and video files (surveillance camera recordings), data stored on computers and computer systems (emails, browsing history), and data stored on telecommunications devices (call lists, location data). At the beginning of a burglary investigation, it is expected that the investigating authority will take action to obtain digital traces out of turn. The same obligation shall apply to due diligence in the search for, seizure and storage of mobile devices and computers in the case of coercive measures taken in the event of the apprehension of perpetrators.[14]

1.1. The new Criminal Procedure Act system of coercive measures for eletronic data

The new On. With its entry into force, it has brought about a significant change in the system of coercive measures, which has made it better able to meet the digital challenges. One of the most important regulatory steps was the already mentioned step that the new Crminal Procedure Act in Section 165. it elevated the electronic data to the rank of independent evidence, together with the wording of its concept. According to it: „Electronic data means the presentation of facts, information or concepts in any form suitable for processing by an information system, including a program which ensures the performance of a function

[8] Section 205. of the New Criminal Procedure Act (2017).
[9] Fantoly Zsanett – Budaházi Árpád: *Büntető eljárásjogi ismeretek. Statikus rész*. Dialóg Campus Kiadó, Budapest, 2019. 123.
[10] Mráz Zoltán: *i.m.,* 96.
[11] Mráz Zoltán: *i.m.,* 97.
[12] Mráz, Zoltán: *i.m.,* 97.
[13] Mráz, Zoltán: *i.m.,* 99.
[14] Mráz, Zoltán: *i.m.,* 100.

by the information system.".[15] As with other means of proof, the existence of legality, professionalism and a closed chain of proof is important for electronic data. Three basic criteria must be met at the stage of the investigation: the original data must not be damaged or altered when the evidence is obtained, the agreement with the original must be proven, and the analysis of the evidence must not alter it. The new Criminal Procedure Act at the same time, it introduced a system of coercive measures based on electronic data, such as the seizure of electronic data (Section 315.), including the retention obligation (Section 316.), and making it temporarily inaccessible (Section 335.). A substantive change in the rules of seizure was made in the new code.[16]

Pursuant to Section 151., the purpose of the seizure is to secure the means of proof or the confiscable property or property subject to confiscation in order for criminal proceedings to be conducted effectively. This coercive measure restricts ownership of electronic data, which can also be ordered by a court, prosecutor's office, and investigating authority. This legal institution has a key role to play in the detection of cybercrime as a means of obtaining and preserving electronic evidence.[17]

There has long been a debate about exactly what should be seized during the procedure, such as the scope of the data specified, or the medium, or the entire information system. It is worth mentioning that the data seizure was first inserted into the old Criminal Procedure Act by Section 21 of an Act in 2013. Prior to that, it was common practice to seize the entire computer (e.g., often with non-criminal hardware, such as a monitor and keyboard), later the hard drive or not, and only a copy was made, and then only the data were seized.[18]

The methods of seizing electronic data are set out in Section 151, which also sets out the order in accordance with the rules of gradation. Seizure may take place: by making a copy of the electronic data, by moving the electronic data, by making a copy of the entire contents of the information system or data medium containing it, by seizing the information system or data medium containing it, or by other means specified by law.[19]

In the first two cases, the contents of the data carrier itself, i.e. the data, are captured by copying or relocating. The methodological issues of seizure are not addressed by law, despite its serious significance. Copying can be done once by the authority inspecting the system on site and copying the data deemed relevant from the information system directly to a medium in the traditional way. However, its application poses a challenge to the forensic principle of both authenticity and completeness. Digital evidence is authentic if it is still possible to determine exactly from which system the data originates, whether an accurate and complete copy of the electronic data has been seized, and whether the data has remained unchanged since its seizure.[20]

2. Digitization in criminal proceedings – proof

Evidence, as a concept rooted in criminal procedure law, is the knowledge of past facts relevant to criminal substantive and formal law by means of lawful means and methods of proof and the proof and recording of those facts by means of evidence. The purpose of the evidence is therefore to obtain the facts and knowledge relevant to the assessment of criminal liability, and its task is to clarify the facts in relation to the committed tort.[21]

2.1. Electronic data as a new means of proof in criminal proceedings

Restricting what is said to electronic data, it should be said that domestic criminal procedure laws are characterized by the inclusion of a list of means of proof. This legislative intention did not mean a closed system for about half a century, an exhaustive list, as the term "in particular" in the relevant provisions referred to. It would follow that means of proof other than those listed could be used. Despite the illustrative list, one view was that the range of possible means of proof was closed, ie the means of proof that could be used in criminal proceedings could be classified into one of the existing types. Tibor Király also had the following opinion about the technical devices that have become known in recent decades. It did not consider it likely that, in the foreseeable future, means of proof would be introduced which would not be included in any of the existing categories. From this point of view, the legislature also thought confidently about the old Be. as it has omitted from the relevant provisions, in connection with the list of means of proof, the aforementioned word ‚in particular', referring to its exemplary nature. In addition to Herke Csongor, Flórián Tremmel and Csaba Fenyvesi do not explicitly consider it acceptable to list the means of proof in an exhaustive way. In their view, due to the development of forensics, more and more methods of proof are gaining independent significance, and at

[15] Section 205. of the New Criminal Procedure Act (2017).
[16] Mezei Kitti: *Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok*. In.: Belügyi Szemle, 2019/10. 27.
[17] Mezei Kitti: *i. m.,* 27.
[18] Mezei Kitti: *i. m.,* 28.
[19] Mezei Kitti: *i. m.,* 28.
[20] Mezei Kitti: *i. m.,* 28.
[21] Gyaraki,Réka Eszter: *i. m.,* 87.

the same time legalized through sui generis procedural regulation.[22]

2.2. Reasons of the self-regulation

If we look for the answer to why it was necessary to declare electronic data as a separate means of proof, highlighting it from the material means of proof and the document, the answer to the law is: "One of the express aims of the law is to establish able to give an answer. The definition of the new means of proof is therefore not an end in itself, and procedural acts, such as special rules on seizure, are based on further detailed rules for electronic data. „Thus, it is possible to conclude that the aim was not to "autonomy" electronic data, it was merely a means to regulate more precisely certain procedural acts and coercive measures.[23]

The legislator justified this need with the following. "The law has taken a stand in favor of separate regulation of electronic data for the reason that electronic data cannot always be treated by analogy with physical things in the regulation of certain criminal proceedings. In cases where common provisions may be made for electronic data and material evidence, the electronic data shall also be treated as material evidence, unless otherwise provided by law.[24]

[22] Róth Erika: *Az elektronikus adat, mint új bizonyítási eszköz megjelenése a büntetőeljárási törvényben*. In.: Miskolci Jogi Szemle, 14. évfolyam, 2. különszám, 2. kötet, 2019. 341–342.
[23] Róth Erika: *i. m.*, 348.
[24] Róth Erika: *i. m.*, 348.

Summary

At the same time, I need to answer the question. Can electronic data really be considered a new means of proof in criminal proceedings? In addition to the classical dogmatic research method, the descriptive as well as the analytical research method helped me in giving the answer. As I had hoped, I came close to the answer. Based on what has been described so far, I would answer the question that it depends.

If I look at the closed dogmatic system of the new Criminal Procedure Act, the answer is definitely yes. After all, the legislator mentions it independently among the means of proof, later defines its specific concept, and creates special rules specifically tailored to electronic data in the system of coercive measures.

However, if I accept the position of Anett Erzsébet Gácsi and Csaba Fenyvesi, that all electronic data and electronic evidence are stored in material means, material means of proof. So computer evidence never exists in isolation, in itself, adding that the old Be. electronic data could also be used in the evidentiary proceedings under its scope, as well as in coercive measures, I have to answer: it cannot be considered as a completely new means of proof. It was merely a tool to define more precisely the rules of its rules of procedure and coercive measures. Which – taking into account the new Be. – the objectives and guidelines of its creation, was in any case an acceptable step on the part of the legislator. In this way, we managed to create a code of procedure that can answer all the questions and challenges of the modern world.