UDC 343.1
DOI https://doi.org/10.24144/2788-6018.2024.02.116

CERTAIN ASPECTS OF CRIMINAL EVIDENCE AND DIGITAL EVIDENCE.

Matis Jakub, JUDr.
External doctoral student in the field of criminal law
Faculty of law of Matej Bel University

Matis Jakub. Certain aspects of criminal evidence and digital evidence.

The evolution of digital technology has revolutionized the landscape of criminal investigations and legal proceedings. This paper delves into the nuanced realm of evidence, with a particular focus on digital evidence, which has become increasingly prevalent in today's digital age. The proliferation of digital information presents both opportunities and challenges for the field of criminal procedure. Recognizing the growing importance of electronic evidence in criminal investigations, the Commission has taken proactive measures to streamline the process of obtaining such evidence. New rules have been introduced to facilitate the acquisition of electronic evidence by judicial authorities. Among these rules are provisions for the creation of a European Evidence Production Order and a European Preservation Order specifically tailored for electronic evidence in criminal cases. Furthermore, providers of electronic services operating within the European Union are now required to appoint a legal representative, further enhancing the accessibility of electronic evidence for legal proceedings. Despite these advancements, the utilization of digital evidence raises complex legal questions and challenges. This paper critically examines the various implications associated with the use of digital evidence, shedding light on issues such as authenticity, admissibility, and the preservation of digital evidence. By analyzing these aspects in depth, the paper aims to provide insights into the multifaceted nature of digital evidence and its implications for criminal procedure.In addition to addressing legal complexities, the paper also seeks to establish a foundational understanding of digital evidence by providing basic definitions and classifications. By elucidating the diverse sources and forms of digital evidence, ranging from emails and transaction records to video recordings and metadata, the paper lays the groundwork for a comprehensive understanding of this evolving field. In conclusion, this paper serves as a comprehensive exploration of the role of digital evidence in contemporary criminal investigations and legal proceedings.

Key words: evidence, digital evidence, Budapest convention, criminal procedure.

Матіс Я. Деякі аспекти кримінальних доказів та цифрових доказів.

Розвиток цифрових технологій докорінно змінив ландшафт кримінальних розслідувань та судочинства. Ця стаття заглиблюється в нюанси доказової сфери, приділяючи особливу увагу цифровим доказам, які стають все більш поширеними в сучасну цифрову епоху. Поширення цифрової інформації створює як можливості, так і виклики для кримінального судочинства. Визнаючи зростаюче значення електронних доказів у кримінальних розслідуваннях, Комісія вжила активних заходів для спрощення процесу отримання таких доказів. Були введені нові правила, що полегшують отримання електронних доказів судовими органами. Серед цих правил – положення про створення Європейського ордеру на отримання доказів та Європейського ордеру на збереження, спеціально розроблених для електронних доказів у кримінальних справах. Крім того, провайдери електронних послуг, що діють на території Європейського Союзу, тепер зобов'язані призначати юридичного представника, що ще більше підвищує доступність електронних доказів для судового розгляду. Незважаючи на ці досягнення, використання цифрових доказів викликає складні правові питання та проблеми. У цьому документі критично розглядаються різні наслідки, пов'язані з використанням цифрових доказів, проливаючи світло на такі питання, як автентичність, допустимість та збереження цифрових доказів. Поглиблений аналіз цих аспектів має на меті дати уявлення про багатогранну природу цифрових доказів та їхні наслідки для кримінального судочинства. Окрім розгляду правових складнощів, у статті також робиться спроба встановити фундаментальне розуміння цифрових доказів шляхом надання базових визначень і класифікацій. Розглядаючи різноманітні джерела та форми цифрових доказів – від електронних листів і записів про транзакції до відеозаписів і метаданих – цей документ закладає основу для всебічного розуміння цієї сфери, що розвивається. Таким чином, цей документ є всебічним дослідженням ролі цифрових доказів у сучасних кримінальних розслідуваннях і судових процесах.

Ключові слова: докази, цифрові докази, Будапештська конвенція, кримінальний процес.

Introduction.

The effective fight against crime and the just punishment of its perpetrators can only be achieved by lawful means, with full respect for the fundamental rights and freedoms of natural and legal persons. Any attempt to apply the 'ends justify the means' approach to criminal law must be rejected as unacceptable and incompatible with the principles of a democratic state governed by the rule of law [1].

The legal regulation of evidence in Slovakia is primarily governed by the Criminal Procedure Code, specifically in its sixth title, which outlines various aspects of evidence in detail. Additionally, other legal norms such as the Charter of Fundamental Rights and Freedoms and the Act on Courts also influence the issue of evidence, alongside court case law, including decisions from the Constitutional Court and general courts. Moreover, international legal sources like the European Convention on Human Rights and decisions from the European Court of Human Rights also play a significant role in shaping the regulation of evidence in Slovakia [2].

In the introduction to the Code of Criminal Procedure there is a reference to evidence, specifically, section 2 defines 20 basic principles, which represent the guiding legal ideas on which the organisational and institutional foundations of the entire criminal procedure are built. These principles are applied either during the entire process, in the pre-trial or in the trial part of the criminal proceedings [3]. In particular, the following principles are linked to the institution of evidence:

- The principle of presumption of innocence,
- The principle of the free evaluation of evidence,
- the principle of proper establishment of the facts of the case,
- The principle of the possibility for the court to take evidence ex officio,
- The principle of immediacy,
- The principle of adversarial procedure,
- The principle of inquiry [4].

Evidence is not only an important, indispensable and indispensable procedural activity in the proceedings before the court, but also the most important procedural activity of the criminal law enforcement authorities in addition to adjudication, as it enables them to establish the factual basis for their decision-making and for further action, so that the purpose of the criminal proceedings may be fulfilled The aim of criminal proceedings is to ensure that offences are properly detected and their perpetrators justly punished according to the law [5].

Evidence is a legally regulated procedure of law enforcement authorities and the court or other persons aimed at seeking, securing, conducting and evaluating knowledge important for the knowledge of facts relevant for the decision on guilt and punishment as well as for the procedure in the proceedings [6].

All facts relevant to the necessary clarification of the facts of the case must be proved. It is the law enforcement authority that determines the framework of the circumstances to be proved. The law enforcement authority must itself assess the circumstances that are relevant and subject to proof in a given criminal case [7].

The court decides what evidence is to be used and taken in evidence and decides only in the case of absolute certainty. This is the criterion of so-called practical certainty, which consists in separating knowledge from probable knowledge, to which the reasonable doubt criterion can be applied. By reasonable doubt we mean uncertainty on the basis of which the prosecuting authority, after a thorough and objective assessment of the evidence, would be indecisive and would not be able to accept whether the facts in question prove that the offence has been committed, or the prosecuting authority would not be able to assess, on the basis of the uncertainty in question, whether the facts proved correspond to the objective reality.

There are several basic terms related to evidence in criminal proceedings :

- **The subject matter of evidence:** A fact to be established by evidence [8].
- **The source of evidence:** All persons and things from which the information is obtained [8].
- **The means of evidence:** The bearer of the information to be obtained by the performance of an evidentiary means.
- **Evidence:** Information, knowledge of law enforcement authorities (the result of evidence), about the subject matter of the evidence, obtained from a means of proof.

In the criminal procedural literature, the subject of evidence is all circumstances and facts important for the accurate establishment of the facts of the case and for the subsequent issuance of a fair decision. Each case is taken individually because it has different circumstances and relies on different evidence, which is why the subject of evidence is individual [9]. The subject matter of the evidence may be understood as the totality of all the facts which are necessary and sufficient for the application of all the rules of substantive law and procedural law [10].

Section 119 of the Criminal Procedure Code defines what is required to be proved in a criminal case: whether an act has been done and whether it has the features of a criminal offence, who committed the act and for what motives, the gravity of the act, including the causes and conditions of

its commission, the personal circumstances of the offender, to the extent necessary for determining the type and amount of the sentence and the imposition of a measure of protection and other decisions, the consequence and the amount of the damage caused by the offence, the proceeds of the offence and the means of committing it, their location, nature, condition and value [11].

Digital evidence.

As a result of the ubiquitous digitalisation of our society, crime is shifting to the online sphere. The fact that the Internet is a medium that knows no borders means that electronic services can be provided from anywhere on earth without requiring the physical presence of the provider in the country where the electronic services are offered. However, the Internet can also be misused as a means of committing or facilitating the commission of crime, including serious crime such as terrorist attacks. Over time, computers are increasingly replacing and supporting a variety of human activities. Along with the introduction of computers, a 'new' phenomenon is emerging, namely the commission of computer-related crime. This phenomenon is often referred to as 'computer crime', 'information technology crime', and in English as 'computer crime', 'cybercrime', 'computer-related crime', 'information technology crime', and 'high-tech crime' [12].

Proving cybercrime is a topical issue globally, and the issue has been addressed by the Council of the European Union and its Justice and Home Affairs Council (JHA), which has stated that cybercrime is becoming more aggressive and confrontational and encompasses an extremely diverse range of criminal activities, including traditional crimes that leave digital footprints followed by digital evidence. Digital evidence represents the future of evidence, not only in criminal proceedings, so it is essential to pay closer attention to it.

Since 2016, there has been a noticeable and significant increase in the use of social media evidence in international and domestic courts [13].

The concept of digital evidence is not directly regulated in Slovak law. Defining digital evidence is not easy as there is currently no clear consensus on its designation, as in professional literature we encounter terms such as "digital evidence", "electronic evidence" or even "computer evidence" [14]. The latter term is often used in a highly restrictive manner, when it refers only to computer-related evidence. The terms "digital" and "electronic" are more expansive and refer to any digital or electronic device that is used to commit a crime. Some authors define digital evidence as information stored or transmitted in digital (binary) form that can subsequently be used in court [15]. In contrast, the European Commission works with the term electronic evidence, which includes various types of data in electronic form, either "content data" or "operational data" that are relevant to criminal proceedings [16].

According to the European Commission's definition, electronic evidence refers to various types of data in electronic form, whether it is "content data" itself, such as IP addresses, emails, photos, videos or usernames, or "operational data " that are relevant for criminal proceedings. These types of data are often indispensable in cybercrime investigations to identify a person or to obtain information about his or her activities.

The Scientific Working Group on Digital Evidence (abbreviated "SWGDE") is a scientific working group on digital evidence that brings together law enforcement, academia, and commercial organizations active in the field of digital forensics globally to develop cross-disciplinary guidelines and standards for recovery, preservation and examination of digital evidence (while subscribing to such a concept) and which defines digital evidence as information with evidentiary value that is stored or transmitted in binary form [17].

A key document of relevance to the acquisition of digital evidence in the context of international crime is the Council of Europe's Budapest Convention on Cybercrime. Although initially focused on the issue of cybercrime, the Budapest Convention has become an indispensable tool in the fight against crime that uses modern technology. The Additional Protocol to this Convention extends its effectiveness to the area of material and procedural jurisdiction, as well as in international cooperation, covering the fight against racist or xenophobic offences.

According to European Council sources, the Budapest Convention is the only binding international instrument in this area. Its dual role is to provide a framework for the implementation of legislative measures to combat cybercrime at the level of the signatory states, while at the same time promoting international cooperation in this area [18].

The Budapest Convention defines the Four Basic Concepts on which the substantive and procedural recommendations and rules of international cooperation are then based. These terms are: computer system, computer data, service provider and operational data.

In addition to definitions and substantive provisions, the Budapest Convention also contains provisions on procedural law and international cooperation.

The specific nature of cybercrime investigations represents one of the most significant challenges facing investigators. The volatility of digital evidence is a crucial factor, as such evidence can be easily corrupted and its recovery is not

always possible. Another important aspect is cooperation with experts, as the acquisition of digital evidence requires specific expertise. It is essential that investigative measures include the digital environment, as digital evidence is not limited to cybercrime, but can also be important in other areas of criminal law.

Article 14 of the above-mentioned Convention establishes the obligation for signatories to take the necessary legislative and other measures to define the powers and procedures identified in this section in order to carry out specific criminal investigations or proceedings, including the collection of evidence in electronic form.

The Convention on Cybercrime has introduced the following specific investigative powers:

– *Expedited preservation of stored computer data,*

– *Expedited preservation and partial disclosure of operational data,*

– *Order to produce computer data,*

– *Search and seizure of stored computer data,*

– *Real-time collection of operational data,*

– *Interception of content data.*

The provisions in question distinguish between *preservation* and *seizure* of electronic evidence. Preservation is understood as a temporary institute to be used when there is a risk of loss or destruction of evidence. It is limited in time to allow the competent authorities to take the appropriate steps to retrieve it. Seizure should only follow preservation [19].

The draft Regulation on cross-border access to electronic evidence contains two types of evidence warrants, namely the European Evidence Warrant for subscriber data and to obtain data for the sole purpose of user identification (Article 4(1) of the draft Regulation on cross-border access to electronic evidence) and the European Evidence Warrant for transaction and content data (Article 4(2) of the draft Regulation on cross-border access to electronic evidence).

With the increasing volume of digital information in the 21st century and its potential value as evidence in criminal proceedings, new opportunities, but also challenges, are opening up. One of the key questions posed by this situation is the possibility of authenticating digital evidence. If the judicial authorities cannot guarantee the authenticity of such evidence, its value in the process of criminal investigation is considerably devalued. This problem has become more pronounced with the advent of 'deepfake' videos, which are sophisticated enough to deceive most viewers.

Another challenge is to ensure the thorough collection and subsequent analysis of digital evidence, which must be rigorously examined and verified. To this end, it is essential to establish a chain of custody (chain of provenance) system, as online platforms such as YouTube often remove metadata, which can make it difficult to determine the value of the evidence itself. Metadata provides information on the time and date of creation of the file, the relevant account and device on which the file was created, and any modifications to the file.

Ideally, metadata should be accessible to aid in verifying potential evidence. Electronic documents, like Word files, frequently contain metadata valuable for confirming their content. This data is auto-generated by software and may also be added by the document's author. Since it's generated automatically, often without user input, it's less likely to be tampered with. For videos, metadata can help identify their location and creator, aiding in investigating relevant events. However, interpreting metadata requires careful evaluation and adherence to basic assumptions, such as trusting that timestamps accurately reflect the device's environment when the information was created and that the metadata hasn't been altered [20].

It is beyond the scope of this paper to provide a detailed overview of all potential sources of digital evidence and their relevance in criminal proceedings. However, we can briefly mention some of the sources that are frequently used for evidentiary purposes:

Master Transaction Records: These include all records of purchases, sales, and other contractual agreements.

Master business records: In addition to transaction records, these include documents and data necessary to comply with legal and regulatory requirements in business relationships.

Email correspondence: Provides important evidence of both formal and informal contacts by suspects or perpetrators.

Records held by third parties: Including cloud service providers.

Personal computers, mobile phones and data media: Containing vast amounts of important data.

Access control logs: Containing records of the issuance of user credentials and access rights to computer systems.

Internal files and logs: Which define the operation of operating systems and programs.

Internet activity logs: Containing records of web accesses and browsing history [21].

In January 2013, the European Commission set up the European Cybercrime Centre, which operates as part of Europol, to effectively combat this specific form of crime. The European Union has a number of instruments at its disposal for obtaining evidence in criminal matters within the framework of judicial cooperation, including the European Union Property or Evidence Seizure Order

and the European Investigation Order. Although the European Investigation Order provides the possibility to access electronic evidence, the European Investigation Order Directive does not contain specific provisions for this type of evidence.

On 17 April 2018, the European Commission presented new rules to allow police and judicial authorities easier and faster access to electronic evidence needed to investigate, prosecute and convict offenders. These new rules are contained in two documents:

Proposal for a Regulation of the European Parliament and of the Council on the European order for the production and preservation of electronic evidence in criminal matters, 17 April 2018 ("the Proposal for a Regulation"),

Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purposes of the taking of evidence in criminal proceedings, 17 April 2018 (hereinafter 'the draft Directive').

The creation of a new instrument focusing on electronic evidence appears to be a better alternative than amending the EIO Directive, as the gathering of electronic evidence entails specific challenges that are not relevant for other investigative measures that are included in the scope of the EIO Directive.

The European Evidence Warrant (Articles 2(1), 4(1), 4(2) of the draft Regulation) is a decision by the issuing authority of a Member State ordering a service provider offering services in the Union and established or represented in another Member State to produce electronic evidence (Funta, 2023, Zefektívnenie cezhraničného prístupu k elektronickým dôkazom). The European Evidence Warrant must be necessary and proportionate for the purposes of the criminal proceedings and can only be issued when a similar measure is available in the issuing State for the same offence in a comparable national situation. The draft Regulation contains two types of orders to produce evidence:

1. **the European Evidence Warrant relating to subscriber data and access data** - can be issued for all offences,

2. **the European Evidence Warrant for transaction and content data** - may only be issued for offences punishable in the issuing State by a custodial sentence of at least 3 years or for offences committed wholly or partly through an information system.

A European Evidence Preservation Order [Article 2(2), Article 4(3) of the draft Regulation] is a binding decision by the issuing authority of a Member State ordering a service provider offering services in the Union and established or represented in another Member State to preserve electronic evidence in respect of a subsequent request for the production of evidence. It may be issued where it is necessary and proportionate to prevent the deletion, erasure, or alteration of data in the light of a subsequent request for the production of that data by means of a mutual legal assistance, a European Investigation Order or a European Evidence Production Order. A European Evidence Preservation Order may be issued for all offences.

The European Evidence Warrant and the European preservation order are issued exclusively in connection with criminal proceedings, whether in their pre-trial or trial phase. These orders may also be issued in cases where they relate to offences for which a legal person may be held liable or punished in the issuing State [22].

In contrast to ambiguous or vague legislation in the Slovak Republic, comparative legal systems have a very precise procedure regarding digital evidence. For example, the U.S. National Institute of Justice (NIJ) in its "Electronic Crime Scene Investigation: A Guide for First Responders" describes a four-step process consisting of the following phases:

1. Collection – Searching for, recognizing, collecting, and documenting digital evidence.

2. Exploration – explaining the origin and meaning of the evidence, searching for information.

3. Analysis – looking at the outcome of examining the significance of digital evidence and the evidential value for a particular case.

4. Reporting – familiarizing the digital evidence obtained [23].

Conclusion.

As digital technology continues to advance, the importance of understanding and effectively utilizing digital evidence in criminal investigations cannot be overstated. In an era where digital interactions are pervasive, digital evidence plays a crucial role in uncovering truth and ensuring justice. By addressing these complexities and providing insights into the evolving landscape of digital evidence, this paper serves as a valuable resource for practitioners, scholars, and stakeholders involved in the field of criminal procedure. It underscores the significance of embracing digital evidence as an essential component of modern investigative practices, highlighting its potential to enhance the integrity and efficiency of criminal proceedings.

REFERENCES:

1. COMENIUS UNIVERSITY IN BRATISLAVA FACULTY OF LAW: PRESS RELEASE*: Zákonnosť a efektivita trestného konania s dôrazom na prípravné konanie - spoločné vyhlásenie.* 2022.
2. KURILOVSKÁ, L., ŠIŠULÁK, S.: *Rýchlosť trestného konania a dokazovanie.* Právny

obzor, 105, 2022, č. 6, s. 507–521. https://doi.org/10.31577/pravnyobzor.2022.6.04/
3. ŠTRKOLEC, M.: *Úvod do trestného práva procesného.* Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2022, 87 s.
4. Act No. 301/2005 Coll., the Criminal Procedure Code, as amended.
5. FRYŠTÁK, M.: *Znalecké dokazování v trestním řízení*. Praha : Wolters Kluwer ČR, 2019, s. 1.
6. ŠIMOVČEK, I.: *Trestné právo procesné*. Plzeň, 2011.
7. IVOR, Jaroslav, et al.: *Trestné právo procesné*. Iura Edition spol. sro, 2010.
8. MIŠKOLCIOVÁ, Iveta.: *Všeobecné východiská dokazovania v trestnom konaní.* Forenzní vědy, právo, kriminalistika, 2021, 6.3: 308–317.
9. BALÁŽ, P. - PALKOVIČ, J.: *Dokazovanie v trestnom konaní*. Bratislava, 2005.
10. HUSÁR, E. a kol.: *Trestné právo procesné*. Bratislava: IURA Edition, 2001. 279 s. ISBN 8089047-04-1.
11. Section 11 of Act No. 301/2005 Coll., the Criminal Procedure Code, as amended.
12. ZÁHORA, J.: *Počítačová kriminalita v európskom kontexte*. In: Justičná revue: časopis pre právnu prax, 2005, roč. 57, č. 2, s. 207 a nasl.
13. KLENKA, M.: *Digitálne dôkazy z otvorených zdrojov*. Pravnik, 2023, 162.6. https://orcid.org/0000-0002-3210-6884.
14. VACCA, R., John: *Computer Forensics: Computer Crime Scene Investigation*, Volume 1, Cengage Learning, s. 7, 2005.
15. NOVAK, Martin, GRIER, Jonathan, GONZALEZ, Daniel: *New approaches to digital evidence acquisition and analysis.*
16. European Commission – Fact Sheet. *Frequently Asked Questions: New EU rules to obtain electronic evidence*, Brussels [online]. 2018 [cit. 01.04.2024]. Available from: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345.
17. SWGDE: *Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science Discipline* [online]. 2014 [cit. 01.04.2024]. Available from: https://www.swgde.org/documents/published- -complete-listing.
18. COUNCIL OF EUROPE. 2022. *Budapest Convention and related standards* [online]. [Cit. 15. 1. 2021] Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention).
19. The Budapest Convention (ETS No. 185) and its Protocols.
20. HONG, Ilyoung.: *International Digital Forensic Investigation at the ICC*. In: BIASIOTTI.
21. SOMMER, Peter: *Digital Evidence, Digital Investigations and E-Disclosure*: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC), Third Edition, s. 25–27 [online]. 2012 [cit. 01.04.2024]. Available from: https:// cryptome.org/2014/03/digital-investigations.pdf.
22. ZÁHORA, Jozef.: *Zaisťovanie digitálnych dôkazov v cezhraničných situáciách*. *Časopis pro právní vědu a praxi*, 2019, 27.1: 49–63.
23. U.S. Department of Justice Office of Justice Programs: (2001) Electronic Crime Scene Investigation: *A Guide for First Responders, written and Approved by the Technical Working Group for Electronic Crime Scene Investigation*, Washington, USA.