UDC 343.1
DOI https://doi.org/10.24144/2788-6018.2025.03.3.19

DIGITAL EVIDENCE AND ITS USE FOR CRIMINAL PROCEEDINGS

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

Matis Jakub. Digital evidence and its use for criminal proceedings.

This paper examines the role and admissibility of digital evidence, particularly data derived from instant messaging applications like WhatsApp and Telegram, in criminal proceedings within the legal context of the Slovak Republic. The focus is on the legal provisions and frameworks under the Slovak Criminal Procedure Code Act, especially regarding the seizure, preservation, and submission of digital data in criminal proceeding. A key aspect of this study is the exploration of how messages and other data from messaging applications are treated as evidence, addressing the complexities of their relevance, authenticity, and credibility in a legal context. In order to establish the admissibility of such evidence in court, the paper delves into essential principles such as the requirement for evidence to be relevant, authentic, and trustworthy. It highlights the fact that courts generally require clear authentication procedures to confirm the authorship of messages, which presents challenges due to the nature of online identities and the potential for manipulation or misrepresentation. The use of screenshots and the specific criteria that ensure they maintain evidentiary value are also discussed, reflecting the practical considerations involved in collecting and presenting digital evidence. Additionally, the paper critiques existing legal provisions in the Slovak Criminal Procedure Code, particularly those that address the seizure and handling of digital data stored on mobile devices and computers. There are notable ambiguities regarding the categorization of mobile devices as computers and the applicable procedures for accessing data from them. The study argues that the current legal framework should be amended to include a clear definition of digital evidence, to standardize the procedures for its collection, preservation, and presentation in court, and to resolve the conflicting interpretations that currently exist in practice. By examining these aspects, the paper contributes to a deeper understanding of how digital evidence is utilized in criminal investigations and legal proceedings, advocating for legislative updates to address the growing importance of digital data in modern criminal cases. Furthermore, it underscores the need for careful consideration of privacy rights and proportionality when dealing with personal information obtained from digital devices and online platforms.

Key words: digital evidence, admissibility, securing digital evidence.

Matіc Якуб. Цифрові докази та їх використання для цілей кримінального процесу.

Ця робота досліджує роль та допустимість цифрових доказів, зокрема даних, отриманих з додатків для миттєвих повідомлень, таких як WhatsApp та Telegram, у кримінальних провадженнях в юридичному контексті Словацької Республіки. Основна увага приділяється юридичним положенням і рамкам, що містяться в Кримінальному процесуальному кодексі Словацької Республіки, зокрема щодо вилучення, збереження та подання цифрових даних у кримінальних провадженнях. Ключовим аспектом цього дослідження є вивчення того, як повідомлення та інші дані з додатків для обміну повідомленнями розглядаються як докази, з огляду на складнощі їх релевантності, автентичності та достовірності в юридичному контексті. Щоб встановити допустимість таких доказів у суді, в роботі розглядаються основні принципи, такі як вимога до доказів бути релевантними, автентичними та надійними. Підкреслюється, що суди зазвичай вимагають чітких процедур автентифікації для підтвердження авторства повідомлень, що створює труднощі через природу онлайн-ідентичностей та потенціал для маніпулювання або перекручування фактів. Також обговорюється використання скріншотів та конкретні критерії, які забезпечують збереження їх доказової цінності, що відображає практичні міркування щодо збору та подання цифрових доказів. Додатково, робота критикує існуючі юридичні положення Кримінального процесуального кодексу Словаччини, зокрема ті, що стосуються вилучення та обробки цифрових даних, збережених на мобільних пристроях та комп'ютерах. Існують значні невизначеності щодо категоризації мобільних пристроїв як комп'ютерів та відповідних процедур доступу до даних з них. Дослідження стверджує, що поточна юридична структура повинна бути змінена, включивши чітке визначення цифрових доказів, щоб стандартизувати процедури їх збору, збереження та подання в суді, а також вирішити існуючі суперечливі тлумачення на практиці. Робота сприяє глибшому розумінню того, як цифрові докази використовуються в кримінальних розслідуваннях та судових процесах, виступаючи за оновлен-

ня законодавства для вирішення зростаючої важливості цифрових даних у сучасних кримінальних справах. Крім того, підкреслюється необхідність ретельного врахування прав на конфіденційність та пропорційності при роботі з особистою інформацією, отриманою з цифрових пристроїв та онлайн-платформ.

Ключові слова: цифрові докази, допустимість, забезпечення цифрових доказів.

I. PROBLEM STATEMENT

Apps such as WhatsApp provide mobile users with the ability to send text messages, voice messages, multimedia files, including images and videos, as well as other types of data in real time, to individuals or groups of contacts. Several years ago, Mark Zuckerberg, whose company Meta (formerly Facebook) owns two of the most prominent communications platforms - WhatsApp and Facebook Messenger - announced that the volume of messages transmitted through these services is three times the global volume of traditional SMS messages. The popularity of instant messaging apps is likely to increase further in the future, which may lead to a significant decline in traditional SMS messaging.

Modern instant messaging applications represent a hybrid model between traditional SMS and traditional instant messaging computer programs. Like SMS, these applications are primarily used on mobile devices and use the infrastructure of wireless networks managed by mobile operators to transmit messages. Unlike traditional SMS, however, instant messaging applications allow users to maintain a single digital identity across multiple client devices, providing a more flexible and integrated communications experience [1].

As a result of the widespread digitalisation of society, there is a significant shift of criminal activity to the online environment. Information and communication technology users are leaving behind large digital traces that can be used to analyse various data such as the location of logins to internet services, the content of messages sent and received, email correspondence, call records and other relevant information.

These digital traces are of crucial importance in a criminal context, in particular when proving a criminal case, as they can provide important evidence concerning potential perpetrators, witnesses or other persons of interest. At the same time, they can provide confirmation of specific criminal activity related to cybercrime, thus contributing to more effective detection of cybercrime [2].

II. RESEARCH OBJECTIVE

The objective of this research is to analyze the legal framework governing the admissibility and acquisition of digital evidence in the Slovak Republic, highlighting shortcomings in the Criminal Procedure Code. It advocates for legislative amendments, including a clear definition of digital evidence, standardized procedures for its handling, and principles for its evaluation. Additionally, the study examines the admissibility of instant messaging as evidence in criminal proceedings, emphasizing relevance, authenticity, and compliance with legal standards.

III. STATUS OF THE PROBLEM AND PRESENTATION OF THE MAIN MATERIAL

Seizing data

We identify three primary institutes in the Slovak Act No. 301/2005 Coll. Criminal Procedure Code (further "Criminal Procedure Code") for seizing data necessary for the purpose of evidence in the field of social networking crimes:

1. **Seizure of a matter important for criminal proceedings pursuant to Article 89 of the Criminal Procedure Code**
2. **Seizure of computer data pursuant to Section 91 of the Criminal Procedure Code**
3. **Seizure of data on telecommunications traffic pursuant to Section 116 of the Criminal Procedure Code.**

Ad 1) The institute of seizure of a thing important for criminal proceedings under Section 89 of the Criminal Procedure Code applies primarily to the seizure of electronic devices through which content may have been published on social networks, electronic communication or other digital interaction may have been carried out. Although the seizure order itself does not primarily serve to seize data, judicial practice has also allowed access to data stored on the seized device as part of this procedural mechanism.

In accordance with the jurisprudence of the Supreme Court of the Slovak Republic, namely Resolution No. 5 Tdo 7/2017 of 23 March 2017, a special order for seizure and access to data on telecommunications traffic pursuant to Section 116(2) of the Code of Criminal Procedure is not required in cases where a mobile phone has already been seized or confiscated as an object of importance for criminal proceedings. This applies irrespective of whether the seizure took place in the context of a search of the home, other premises or land or during a search as a material trace.

Ad 2) Provision of Section 91 of Act No. 301/2005 Coll. of the Code of Criminal Procedure regulates the **storage, release and withdrawal of computer data**:

"Where the preservation of stored computer data, including operational data which has been stored by means of a computer system, is necessary for the purposes of the evidence, the President of the Chamber and, before the commencement of the prosecution or in the preparatory proceedings, the public prosecutor may issue an order, which must also be justified by the facts, to the person in whose possession or under whose control such data is held or to the provider of such services, requiring him or her to

a) preserve and maintain the integrity of such data,

b) enable a copy of such data to be made and retained,

c) prevent access to such data,

d) remove such data from the computer system,

e) release such data for the purposes of evidence." [3].

In the application practice of law enforcement authorities and courts, ambiguities arise regarding the interpretation of the provision of Section 91 of the Criminal Procedure Code, in particular in relation to its relation to data stored in mobile phones and similar devices. A key aspect in the interpretation of this provision is the phrase *"storage of stored computer data, including operational data stored by means of a computer system."*

In practice, the prevailing view has been that data stored on smartphones cannot be considered computer data within the meaning of the provision. Therefore, their seizure is not subject to the regime of Article 91 of the Code of Criminal Procedure, but the procedure under Article 90 of the Code of Criminal Procedure, which regulates the general seizure of a thing, is sufficient [4].

In connection with the issue of seizure of digital data, reference may be made to part of the reasoning of the judgment of the Supreme Court of the Slovak Republic (Case No. 2To 9/2014 of 26 November 2014). In that decision, the Court rejected the objection according to which it should have been necessary to apply the procedure under Section 90 (now Section 91) of the Criminal Procedure Code (order for preservation and surrender of computer data) for the expert examination of mobile phones due to their operating system, stating that the procedure under Section 89 and Section 91 (now Section 90) of the Criminal Procedure Code (surrender or withdrawal of the item) was sufficient. This view was also shared by the Specialised Criminal Court.

The Supreme Court of the Slovak Republic concluded that despite the technical similarities between mobile phones and computers, these devices cannot be considered identical, which is also reflected in their commercial categorisation as different types of goods. On that basis, the Chamber of the Supreme Court of the Slovak Republic held that data stored by means of a mobile phone cannot be considered as data stored by means of a computer system within the meaning of Section 90 (now Section 91) of the Code of Criminal Procedure.

Reference may be made to the resolution of the Constitutional Court of the Slovak Republic, case no. II ÚS 78/2019, which rejected the constitutional complaint of a journalist cooperating with Ján Kuciak, whom the NAKA investigator, who was conducting a criminal prosecution for a particularly serious crime of murder of Ján Kuciak, after her interrogation, asked to allow her to make a copy of the data stored in her mobile phone and after her refusal, he delivered to her the order of the prosecutor to preserve the computer data pursuant to Section 90 (1) (b) of the Code of Criminal Procedure and warned her of the possibility of imposing an orderly fine, respectively. The phone was subsequently handed over and a report was made. In the proportionality test, which examined the legality of the interference, the legitimacy of the aim and the proportionality of the interference, the Constitutional Court concluded that the procedure of the CID in the case in question was in accordance with the Constitution, with reference to the seriousness of the criminal activity under investigation and the initial stage of the investigation, and the proportionality of the interference as a result of the sequence of the use of the institutes, since the institute of surrender and preservation of computer data takes precedence over the institute of surrender and deprivation of property, since it is a milder means of interfering with the applicant's constitutional rights. In this decision, the Constitutional Court expressed the opinion that a smart mobile phone has the nature and character of a computer and contains computer data, despite the decision of the Supreme Court Case No. 5Tdo 7/2017 of 23.03.2017, if it is necessary to secure data from the phone other than data related to calls and SMS messages (communication through data transmission using applications such as Viber, WhatsApp, Messenger, Threema, Slack...) from smart mobile phones, the procedure under Section 90 of the Criminal Procedure Code can be used.

This procedure shall apply in particular to obtain relevant information from the *operator of the platform concerned.* This data, usually in the form of system logs, may provide a detailed overview of the activity on a particular user account, including log-in time logs, IP addresses or other identifiers allowing the identification of the actual user of that account [5, p. 438].

Ad 3) While the previous point relies on obtaining information from the operator of the platform in question, the institute of seizure of data on telecommunications traffic under Article 116 of the Criminal Procedure Code relies in particular on obtaining information from the *provider of the internet connection* for the electronic device on the amount, timing and addressability of the data transmitted from the device that was to be used to publish hate speech on the social network to the servers operating the social network. This data may allow the specific data stream that transmitted the hate speech from the electronic device to the social network server to be identified. In view of the interference with the subject-matter of the communication secret, it must be duly justified [6, p. 438].

Digital evidence

Section 119(3) of the Criminal Procedure Code says that anything that can contribute to the proper elucidation of the case and which has been obtained from evidence under this Act or under a special law may be used as evidence.

The ***admissibility*** of evidence is the legal capacity of a particular piece of evidence to support or refute allegations or claims in a legal proceeding and cannot be rejected a priori by the court. This principle is based on the right to a fair trial, which is enshrined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. In assessing the admissibility of evidence, it is necessary to take into account its nature and the circumstances in which it was obtained [7, p. 255].

A key criterion for the admissibility of evidence is the lawfulness of its acquisition. The admissibility of evidence is a broader concept than its legality - although evidence obtained in violation of the law is always inadmissible, not all inadmissible evidence must also be illegally obtained.

Burda stresses that illegally obtained evidence cannot, in principle, be admissible in criminal proceedings unless its illegality can be remedied and subsequently eliminated (so-called relatively ineffective evidence).

On the other hand, the possibility of using illegally obtained evidence in certain circumstances. He refers to Article 119(4) of the Code of Criminal Procedure, which excludes the admissibility of illegally obtained evidence, but not absolutely. In order for evidence to be inadmissible, the illegality must be connected with the use of coercion or the threat of coercion. It follows that the mere illegality of evidence does not automatically render it inadmissible [8, p. 23].

Digital evidence is a dynamic category of evidence that evolves in line with technological advances. In the past, "computer evidence" in criminal proceedings was mainly seen as printed output from a computer, which was considered to be documentary evidence. Today, however, the concept of digital evidence encompasses a wide range of data stored, generated, processed or transmitted through digital and electronic devices [9].

The terms "digital evidence" and "electronic evidence" are often used synonymously in professional practice, but with slight differences. Digital evidence is generally defined as information stored or transmitted in digital (binary) form that can be used in legal proceedings. The European Commission is working with the broader concept of 'electronic evidence', which encompasses different types of data in electronic form, dividing it into content data (e.g. text, images, videos) and operational data (e.g. IP addresses, timestamps, metadata of communications) which can be crucial for criminal investigations [10].

A digital evidence can be defined as any data that can serve as evidence, regardless of whether it is stored, generated, processed, or transmitted by an electronic device.

Key Sources of Digital Evidence:

- Main transaction records – purchases, sales, contractual agreements.
- Emails – communication of suspected individuals.
- Personal computers and mobile devices – contain crucial digital evidence.
- Cloud storage – data stored by third parties.
- Data storage media – USB drives, external disks, CDs/DVDs.
- Access and internet activity logs – records of logins and web browsing.

Message as an evidence

Messages from apps such as WhatsApp, Signal or Telegram have a high evidentiary value in criminal proceedings because they may contain direct confessions, incriminating information or communications between perpetrators. However, their use raises questions about privacy, telecommunications secrecy and the protection of the confidentiality of communications.

When collecting such evidence, public authorities must be guided by the principles of proportionality and necessity, and their interference with privacy must be lawful, *legitimate* and *proportionate*.

In order to be used in criminal proceedings, messages from instant messaging applications must meet the following basic criteria:

1. **Relevance:** the evidence must be materially relevant, i.e. it must relate to the subject matter of the proceedings. If the messages do not provide direct evidence of the guilt or innocence of the defendant, they may be excluded by the court.
2. **Authenticity:** in order for messages to be used as evidence in criminal proceedings, the sender must be identified. Challenges in this area include the use of disposable emails or phone numbers that make it difficult to associate an account with a specific person, dynamic IP addresses that change and can be shared by multiple devices, or logging in from different devices.
3. **Credibility:** if there is a possibility of manipulation of the messages, for example by editing the conversation, the court may question their credibility.
4. **Originality requirement:** In most cases, screenshots of messages are accepted as evidence, but the quality and form of the recording may affect their probative value. For example, the Supreme Administrative Court of the Czech Republic has stated that when capturing the content of a website, a printout of the text without graphic elements is sufficient for evidentiary purposes, but if the evidence is to include visual elements, it must be preserved in its original form. This principle can also be applied to messages from apps - for example, if the message contains photographs or emoticons that have testimonial value, it must be captured in such a way that these elements are not distorted or removed [11].

The mere recording of a message ("screenshot" or "printscreen") in a criminal complaint containing the name of the author of the post is not (even after verifying the actual existence of the post on the social network) a sufficient basis on its own for the issuance of a charging order against the person who is identified as the author of the post in the criminal complaint. The law enforcement authorities should observe the principle of restraint and verify whether the suspect actually has a profile that identifies the social network as the author of the message or post. The profile may have been purposely created by the perpetrator in someone else's name on purpose [12].

IV. CONCLUSION

The purpose of this contribution was to provide a brief overview of the legal regulation concerning the admissibility of digital evidence and its acquisition within the framework of the Slovak Republic. Given the numerous shortcomings in the Slovak Criminal Procedure Code regarding digital evidence, we are of the opinion that an amendment to the Criminal Procedure Code is necessary, including the introduction of a definition for digital evidence, in order to prevent differing interpretations by law enforcement authorities and courts. Additionally, it is essential to provide a clear procedure for the collection, handling, storage, and submission of such evidence. It is also crucial to more specifically define the principles that govern the evaluation of digital evidence in criminal proceedings.

We also examined the admissibility of instant messaging as evidence in criminal proceedings. For evidence from instant messaging apps to be admissible, it must be relevant, authentic, and trustworthy, aligning with the best evidence rule and not posing undue risks of unfair prejudice. Its relevance is determined by its connection to the case. Courts require the submitting party to provide relevant proof, meaning not all evidence from these apps is automatically admissible. Authentication is key for admissibility, as text messages must be verified to establish authorship. For example, a defendant's name in a message alone is not enough; it must be proven that the message came from an account the defendant uses. Screenshots are generally accepted as admissible duplicates. The study did not exhaust the entire problem and therefore leaves room for further research with respect to future case law of the courts.

REFERENCES

1. FUNTA, R.: *Mobilné aplikácie ako dôkaz v trestnom konaní?*, 2021. URL: https://www.judikaty.info/cz/document/article/4982.
2. HALAS, N.: Digitálny dôkaz v trestnom konaní, 2022. URL: https://naos-be.zcu.cz/server/api/core/bitstreams/b46ed43e-47b1-418d-a945-81c057523329/content.
3. Section 91 of Act No. 301/2005 Coll. Criminal Procedure Code.
4. HALAS, N.: K uchovaniu a vydaniu počítačových údajov z obsahu mobilných telefónov v trestnom konaní; Justičná revue, 72, 2020, č. 6-7, s. 803–811.
5. BIROŠ, M.: *Zabezpečovanie dôkazov zo sociálnych sietí v oblasti nenávistných prejavov*, [online]. 2024. URL: https://unibook.upjs.sk/sk/pravnicka-fakulta/1233-kosicke-dni-trestneho-prava-2024.html.
6. BIROŠ, M.: *Zabezpečovanie dôkazov zo sociálnych sietí v oblasti nenávistných prejavov*, [online]. 2024. URL: https://unibook.upjs.sk/sk/pravnicka-fakulta/1233-kosicke-dni-trestneho-prava-2024.html.
7. ŠIMOVČEK, I.: *Teoretické a praktické problémy dokazovania.* Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 200, s. 255.

8. BURDA, E.: *Teoretické a praktické problémy dokazovania.* Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou konanej dňa 15. decembra 2008. Bratislava: BVŠP, 2008, s. 23.
9. NOVAK, M. – GRIER, J. – GONZALEZ, D.: N*ew approaches to digital evidence acquisition and analysi*, [online]. 2018. URL: https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis.
10. European Commission – Fact Sheet. Frequently Asked Questions: *New EU rules to obtain electronic evidence, Brussels.* [online]. 2018 URL: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_334.
11. FUNTA, R.: *Mobilné aplikácie ako dôkaz v trestnom konaní?*, 2021. URL: https://www.judikaty.info/cz/document/article/4982/.
12. BIROŠ, M.: *Zabezpečovanie dôkazov zo sociálnych sietí v oblasti nenávistných prejavov*, [online]. 2024. URL: https://unibook.upjs.sk/sk/pravnicka-fakulta/1233-kosicke-dni-trestneho-prava-2024.html.