УДК 343.140

Iryna Shulhan
Lviv Polytechnic National University,
PhD.,
Associate Professor of the Department of
Administrative and Information Law
of Institute of Jurisprudence, Psychology and Innovative Education
iryna.i.shulhan@lpnu.ua
ORCID ID: https://orcid.org/0000-0002-9623-3495

ELECTRONIC EVIDENCE AS EFFECTIVE TOOLS OF PROVING IN CRIMINAL PROCEEDINGS

http://doi.org/10.23939/law2023.37.202

The process of proving is carried out by competent participants of criminal trial in order to establish the truth in criminal proceedings and is an important component of the proceeding. Proving is carried out in compliance with the statutory procedure for criminal proceedings in general, the order of the execution of certain procedural actions and the adoption of procedural decisions, that is within the limits of the criminal procedural form. The modern concept of criminal proceedings is aimed at establishing additional guarantees of observance of the participants' rights at each stage. The process of proving should be clearly regulated by criminal procedure legislation to ensure the rights of a person in criminal proceedings.

The rapid development of the latest information technologies and a significant increase in the number of legal relations in the plane of the information space objectively affected the features of the criminal process. In particular, this applies to such an important category as sources of evidence. In modern conditions of widespread use of information technologies, electronic media are an important and informative source of evidence in criminal proceedings.

From theoretical and practical perspectives an important task for scholars is to regulate at the legislative level the methods and procedural proceedings for the legal collection of digital information relevant to criminal proceedings and its further use in compliance with the principles of relevance, admissibility, reliability and sufficiency.

The peculiarities of collecting, processing and recording digital evidence are analyzed in the article. It is emphasized that the collection of evidence contained on electronic media can be done by removing the media or information system and by copying the information stored on the corresponding electronic media. The advantages and disadvantages of using digital evidence collection methods are analyzed. Emphasis is placed on the importance of observing the procedural and technical aspects of obtaining information stored on electronic media in order to ensure the possibility of using such information as evidence during criminal proceedings.

Key words: evidence, prooving, collection of evidence, electronic media, electronic evidence, digital evidence.

Electronic evidence as effective tools of proving in criminal proceedings

Formulation of the problem. Evidence and prooving are the basis of any process. The effectiveness of criminal proceedings in court and the speed of achieving the goal of justice depend on the quality and completeness of the evidence base collected during the pre-trial investigation. The pre-trial investigation of criminal misdemeanors, which is carried out in the form of an inquiry, is also inextricably linked with prooving, which in the specified procedure has its own peculiarities due to its specificity. The study of the institution of prooving at the stage of inquiry is of great importance in view of the possibility of simplified proceedings regarding criminal misdemeanors established in the legislation, which provides for the possibility of a court passing a verdict without examining the evidence in a court session or on the basis of their partial examination.

Evidence in a criminal trial evolves with the person. The modern level of the technical process has affected the fact that every criminal proceeding contains evidence that is presented in electronic form.

Evidence in electronic form became especially relevant in connection with the military aggression of the Russian Federation against Ukraine, because since 2014, investigations into proceedings committed in temporarily occupied territories can only be conducted remotely. Today, the use of electronic evidence is becoming even more relevant.

Analysis of the problem research. Such scientists as Hutsaliuk M., Havlovskyi V., Kalancha I., Orlov Yu., Pashyn S., Samoilov S., Sergeiev M., Khakhanovskyi V., Khyzhniak Ye., Cherniavskyi S., Sheifer S. devoted scientific works to the study of the problems of collecting and procedurally securing electronic (digital) evidence.

The purpose of the article is to analyze the features of collection, processing and recording of evidence contained on electronic media; to focus attention on compliance with the basic principles regarding propriety, admissibility, reliability and sufficiency of digital evidence.

Presentation of the main material. Proving in criminal proceedings as a type of cognitive process is considered as mental activity that proceeds in accordance with the laws of logic, in specific logical forms. It should be emphasized that the concepts of evidence and prooving in criminal proceedings are normatively enshrined in Article 65 of the Criminal Procedure Code of Ukraine (hereinafter the Criminal Procedure Code of Ukraine), which states that evidence in criminal proceedings is factual data obtained in the manner prescribed by this Code, on the basis of which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances that are important for criminal proceedings and are subject to prooving [1].

Today, in the course of proving in criminal proceedings the following evidence can be used: photos, audio-, video- records of electronic communication (telephone conversations), various computer data, electronic correspondence (sms-messages, e-mail, messengers), network traffic, data from streaming services, information about the location of objects, geolocation, social network data, IP address and network port data, electronic digital signatures, electronic time stamps and much more.

The rapid development of the latest information technologies led to the emergence of new types of offences and changes in the existing forms of crime. Crimes committed with the help of modern technologies are called cybercrimes [2, p. 10]. The growth rate of crime in the global computer network is the highest compared to other types of crime [3, p. 113].

Cybercrimes are committed from anywhere on the planet (provided there is access to the Internet) and, in fact, without leaving home. When investigating such crimes, conventionally “classic” evidence, such as witness statements, paper documents, and identification protocols, are actually absent.

As it is stated by scholar Pavlova Yu., electronic evidence are specific as it is information in its pure form. It does not have a material form of existence, is easily subjected to destruction and modification, has an inseparable connection with the technical medium of information and at the same time is easily moved in space with the help of telecommunication networks. Electronic evidence has a technical nature of its

origin, and therefore the interpretation of its content is carried out with the help of special software tools [4, p. 77].

Scientists actively discuss not only the essence of traces of crimes in the field of information technology use, but also their names. The following names of traces of this category are proposed: computer traces, virtual traces, electronic-digital, informational, computer-technical, etc. [5, p. 169]. The name "electronic evidence" seems to be the most successful and the one that adequately reflects the essence of traces of crimes of the specified category.

Electronic evidence is any evidence in criminal proceedings that can be obtained in electronic form. Electronic evidence is obtained with the help of electronic devices, computer media, as well as computer networks, including via the Internet. They become available for human perception after processing by means of computer technology [6, p. 6].

Along with the concept of "electronic evidence", the concept of "digital evidence" is often used. Since these concepts have not yet been defined at the legislative level, they are used in parallel.

The initial procedure of processing electronic media (EM) involves the identification, collection, extraction and preserving of potential digital evidence. Digital evidence can be volatile in nature. They may change, deteriorate, or be destroyed during improper handling or inspection. Therefore, persons working with digital evidence must be competent and guided by clear requirements to avoid risks. Mishandling digital devices can render potential digital evidence contained on them unusable.

The fundamental principle for processing sources of potential digital evidence should be to minimize the processing of the original digital devices and potential digital evidence, and to document and explain any changes to digital information. With regard to evidence, experts should not act outside their competence. All actions and processes must be documented in accordance with legal requirements, especially if this may lead to the inevitability of changes.

In order to acquire the status of evidence, information must meet four characteristics (principles): appropriateness, admissibility, reliability, sufficiency. Digital evidence is appropriate if it provides an opportunity to prove or disprove the circumstances to be proven. The main task of the admissibility requirement is to guarantee that the digital evidence is obtained in the manner and from the sources directly provided for by the Code of Criminal Procedure of Ukraine. The reliability of evidentiary information means that it correctly and adequately reflects the material and immaterial traces of the committed illegal act. The concept of sufficiency assumes that a sufficient amount of potential digital evidence should be collected to ensure the possibility of reaching a conclusion about the presence or absence of the circumstances of the case that are included in the subject of prooving [7, p. 4, 5].

If electronic storage devices are discovered in the course of investigative (detective) actions, the collection of evidence - the information contained on the storage device – can be carried out in two ways:

1) by removing the device or information system;

2) by copying information stored on the appropriate electronic medium (in this case, the issue of data fixation from cyberspace is not considered) [8, p. 336].

The above methods of gathering evidence have both advantages and disadvantages and certain application limitations.

The traditional method of collecting evidence in criminal proceedings is the seizure of material objects, in particular, electronic media and information systems. However, physical extraction is not always technically possible. For example, the difficulty of extracting information systems can be caused by their bulkiness, the threat of suspending production processes or the danger of losing access to information (in particular, if it is impossible to successfully start decryption later in the event that the system with active encryption is turned off).

Therefore, an alternative to the removal of the digital information carrier as a method of gathering evidence can be the production of a copy of the digital information. The relevant procedural possibility has been recorded in the Criminal Procedure Code of Ukraine since 2017. According to Part 4 of Article 99 of the Criminal Code of Ukraine copies of information, including computer data, contained in information

(automated) systems, electronic communication systems, information and communication systems, computer systems, their integral parts, made by an investigator, a prosecutor with the involvement of a specialist, are recognized by the court as the original of the document. Backup copies of such data are allowed to be stored separately from the materials of criminal proceedings (Part 3 of Article 107 of the Criminal Procedure Code of Ukraine) [1].

In addition, in accordance with Part 1 of Article 159 of the Criminal Procedure Code of Ukraine, temporary access to material objects and documents is carried out exclusively by removing a copy of information, if access was granted by the court to electronic information systems or their parts (computers) or mobile terminals of communication systems (telephones).

The described situations form a system of procedural scenarios that require the production of a copy of electronic information or electronic information carrier during criminal proceedings.

In order to identify and record information regarding the circumstances of the commitment of a criminal offense, the investigator and prosecutor conduct an inspection of the area, premises, things, documents and computer data. The review of computer data is carried out by the investigator, the prosecutor by displaying in the review protocol the information they contain in a form suitable for perceiving their content (using electronic means, photography, video recording, shooting and/or video recording of the screen, etc. or in paper form) (Article 237 of the Criminal Procedure Code of Ukraine).

If the investigator, the prosecutor, based on the results of the analysis of the operational situation during investigative (search) actions or due to the procedural necessity, made a decision to copy the information stored in the electronic information carrier, to ensure the possibility of using such information as evidence during criminal proceedings, it is necessary to observe two aspects: procedural and technical.

The procedural aspect consists in the investigator's or prosecutor's compliance with the requirements of Part 4 of Article 99 of the Criminal Procedure Code of Ukraine regarding the need to involve a specialist. At the same time, it is worth noting that the formal fulfillment of the requirement of the Criminal Procedure Code of Ukraine regarding the involvement of a specialist does not guarantee the identity of the copy of the original information. The specialist engaged by the prosecution must have the necessary knowledge and skills in the field of information technology and be able to correctly implement the copying process, which must include verification (checking) of the integrity and authenticity of information with the provision of appropriate guarantees. Attention should be paid to the fact that non-compliance with the technical aspects of guaranteeing the integrity and authenticity of information can discredit the produced copy.

Thus, it becomes obvious that there is necessity to observe the technical aspect of the information copying process, the importance of which is difficult to overestimate. The admissibility of the backup copies created in this way without the participation of a specialist is recognized by the court, taking into account the exceptional grounds provided for in Clause 1, Part 5 of Article 99 of the Criminal Procedure Code of Ukraine, when the original document is lost or destroyed through no fault of the party providing it [1].

At the same time, given the shortcomings of the criminal procedural law, the heterogeneous practice of law enforcement and the lack of special knowledge in the field of information technology, a significant number of investigators and prosecutors cannot always organize the correct production of a copy of electronic information, which leads to the loss of evidence (flaws in collection and storage) or recognition of collected evidence as inadmissible (violation of procedural or technical norms by participants in investigative (search) actions) [7, p. 4].

Part 2 of Article 93 of the Criminal Procedure Code of Ukraine contains an indication of another method of collecting electronic evidence – it can be demanded from state authorities, local self-government bodies, officials and individuals, enterprises, institutions and organizations. Internet service providers (ISPs) and mobile operators are the enterprises that play a key role in ensuring the circulation of electronic images and have the technical capabilities to preserve them. At the same time, their relations with investigative bodies are not procedurally regulated today, which leads to numerous misunderstandings,

unjustified seizure by investigators of network computer equipment from providers, which leads to violations of the rights of Internet users and to the recognition by the court of the obtained evidence as inadmissible, and also creates providers' reluctance to provide information to law enforcement agencies [3, p. 119].

In the context of the analyzed issues, it is worth emphasizing the importance of making changes to the current criminal procedural legislation in connection with the need to clarify the terminology and improve the provisions on temporary access and seizure of information and telecommunication systems. The changes should be aimed at preventing arbitrary interpretation of the norms regarding the concept of electronic evidence and abuses in the specified area.

Conclusions. In the modern conditions of the development of innovative technologies, evidence contained on electronic media is an important source of evidence in criminal proceedings. The Criminal Procedural Code of Ukraine provides for two main methods of collecting information contained on electronic media – by removing the media or information system and by copying information. Provided that the procedural and technical aspects of collecting electronic evidence are observed, they acquire the value of effective tools of proving.

Compliance with the procedural form of electronic information retrieval is ensured by the investigator or prosecutor with the involvement of a specialist. Copying is an effective way of obtaining evidence from a suitable electronic medium. In order to ensure the recording of information and the use of a copy of the information during the trial, it is necessary to ensure compliance with the requirements of Part 4 of Article 99 of the CCP of Ukraine. The need to comply with the technical aspect of the information copying process becomes obvious.

Digital evidence is based on the basic principles inherent in all evidence – propriety, admissibility, reliability and sufficiency. These principles are important because they make it possible to establish circumstances that are subject to prooving in criminal proceedings.

REFERENCES

1. **Kryminalnyi protsesualnyi kodeks Ukrainy.** [Criminal Procedure Code of Ukraine] : Zakon Ukrainy No. 4651-VI vid 13.04.2012 r. URL : http://zakon2.rada.gov.ua/laws/show/4651-17 (data zvernennia 07.02.2023).

2. Shylo O. (2016). **Problemni pytannia dosudovoho rozsliduvannia zlochyniv, uchynenykh iz zastosuvanniam kompiuternykh tekhnolohii ta/abo vykorystanniam merezhi internet.** [Problematic issues of pre-trial investigation of crimes committed with the use of computer technologies and/or the use of the Internet]. Mizhnarodni standarty z kiberbezpeky ta yikh zastosuvannia v Ukraini (materialy "kruhloho stolu" m. Kharkiv, 19 kvit. 2016 roku). Kharkiv : Pravo, P. 10–13.

3. Cherniavskyi S., Orlov Yu. (2017). **Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni.** [Electronic display as a source of evidence in criminal proceedings]. Visnyk kryminalnoho sudochynstva. No. 2. P. 112–124.

4. Pavlova Yu. (2017). **Osoblyvosti zbyrannia ta protsesualnoho zakriplennia elektronnykh dokaziv u tsyvilnomu sudochynstvi.** [Peculiarities of collecting and procedurally securing of electronic evidence in civil proceedings]. Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Vyp. 4. T. 1. P. 76–80.

5. Avdieieva H., Storozhenko S. (2017). **Elektronni slidy: poniattia ta vydy.** [Electronic traces: concepts and types]. Visnyk LDUVS im. E. O. Didorenka. No. 1 (77). P. 168–175.

6. Hutsaliuk M., Havlovskyi V., Khakhanovskyi V. (2020). **Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh.** [The use of electronic (digital) evidence in criminal proceedings] : metod. Rekom / za zah. red. Korneika V. Vyd. 2-he, dop. Kyiv : Vyd-vo Nats. akad. vnutr. Sprav. 104 p.

7. **Metody zakhystu. Nastanovy dlia identyfikatsii, zbyrannia, zdobuttia ta zberezhennia tsyfrovykh dokaziv.** [Methods of protection. Guidelines for the identification, collection, acquisition and preservation of digital evidence]. Kyiv : DP "UkrNDNTs". 37 p.

8. Harkusha A. (2021). **Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty.** [Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects]. Yurydychnyi naukovyi elektronnyi zhurnal. No. 1 8. P. 336–339.

Дата надходження: 01.12.2022 р.

Ірина Шульган
Національний університет "Львівська політехніка",
кандидат юридичних наук,
доцент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
iryna.i.shulhan@lpnu.ua
ORCID ID: https://orcid.org/0000-0002-9623-3495

ЕЛЕКТРОННІ ДОКАЗИ – ДІЄВІ ІНСТРУМЕНТИ ДОКАЗУВАННЯ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Процес доказування здійснюється компетентними учасниками кримінального процесу з метою встановлення істини у кримінальному провадженні і є його вагомим складовим елементом. Доказування відбувається з дотриманням визначених законом порядку кримінального провадження загалом, виконання окремих процесуальних дій та прийняття процесуальних рішень, тобто у межах кримінальної процесуальної форми. Сучасна концепція кримінального процесу спрямована на встановлення додаткових гарантій дотримання прав його учасників на кожному етапі. Процес доказування повинен бути чітко регламентований кримінальним процесуальним законодавством задля забезпечення прав особи у кримінальному провадженні.

Стрімкий розвиток новітніх інформаційних технологій та збільшення кількості правовідносин у площині інформаційного простору об'єктивно позначилися на особливостях кримінального процесу. Зокрема, це стосується такої важливої категорії, як джерела доказів. У сучасних умовах широкого застосування інформаційних технологій електронні носії інформації є важливим та інформативним джерелом доказів у кримінальному провадженні.

Важливим завданням науковців, із теоретичного та практичного боку є врегулювання на законодавчому рівні способів та процесуальних процедур законного збирання цифрової інформації, що має значення для кримінального провадження, та подальшого її використання, з дотриманням принципів належності, допустимості, достовірності та достатності.

Проаналізовано особливості збирання, опрацювання та фіксації цифрових доказів. Наголошено, що збирання доказів, які містяться на електронних носіях, може відбуватися шляхом вилученням носія або інформаційної системи та шляхом копіювання інформації, що зберігається на відповідному електронному носії. Проаналізовано переваги та недоліки застосування способів збирання цифрових доказів. Акцентовано на важливості дотримання процесуального та технічного аспектів отримання інформації, що зберігається на електронних носіях, для забезпечення можливості використання такої інформації, як доказу під час кримінального провадження.

Ключові слова: докази, доказування, збирання доказів, електронні носії інформації, електронні докази, цифрові докази.