

Electronic Document As A Source In Criminal Proceedings

Oleksandr Manzhai[†], Andrii Lysenko[†], Iryna Burlaka^{††}, Viktoriia Vintsuk[†], Ruslan Chycha[†]

[†]Kharkiv National University of Internal Affairs, Ukraine

^{††}Judge in Kharkiv Court of Appeal, Ukraine

Summary

The use of electronic documents and other types of digital information as evidence in criminal proceedings has its own characteristics, which are discussed in this paper. The purpose of the study is to consider the problems of using electronic documents as evidence in criminal cases, which arise both in the theory of criminal procedure and in investigative and judicial practice. Unfortunately, the legislator does not always keep up with the development of the information society, as a result of which the regulation of legal relations is incomplete. The importance of using electronic documents in criminal procedure legislation is determined. The main definitions of the electronic document used in regulations and scientific works of scientists are considered. The main approaches to the term "electronic document" are analyzed and the necessity of using this term is substantiated, the definition of an electronic document as a source of evidence is given. It is proposed to allocate an electronic document as a separate source of evidence.

Keywords: Evidence, Electronic evidence, Digital evidence, Electronic document

1. Introduction

Decades ago, the use of electronic documents in various spheres of human life was rather exotic. However, the results of scientific and technological progress have led to the emergence of various electronic devices and prompted the gradual replacement of paperwork by electronic, which is dictated by the undeniable advantages of the latter, including simplification of search, storage, change of information. Electronic means of communication, electronic documents, electronic messages are increasingly being used in various legal relationships.

Today the problem of legal regulation of the use of electronic documents in criminal proceedings is relevant. Recently, in the practice of criminal proceedings, the issue of informatization is becoming increasingly important, but the problem of improving the criminal process remains insufficiently studied in legal science. Investigation of criminal cases is sometimes impossible without proper information and analytical support. Currently, law enforcement agencies regularly turn to numerous information systems to obtain the necessary information, most often they turn to collect materials describing the accused. The planned transition from classic paper

document management to electronic document management meets modern requirements and trends in the development of the information society and will ensure the rapid exchange of information resources. Today it is important to consolidate the concept of electronic evidence in the Criminal Procedure Code of Ukraine and the formation of methods for their study.

2. Theoretical Consideration

The informatization of public life objectively affects the peculiarities of the criminal process. In particular, this applies to such an important category as sources of evidence. The Criminal Procedure Code of Ukraine contains a list of crimes committed in the field of use of electronic computers (computers), systems and computer networks and telecommunications networks. Spyware, computer viruses, programs for unauthorized access, etc. can be specific tools for committing crimes in this case. And for the study of such evidence requires special methods and tools, programs. At the same time, there is the problem of examining such evidence in court. In addition, electronic evidence may threaten to violate the human right to privacy. Electronic media cause the existence on it of a large amount of personal information that is not relevant to criminal proceedings. All these issues are quite relevant and need thorough research and regulation at the legislative level.

Electronic evidence today is a symbol of evidence, the content of which is presented in electronic form. This state of affairs persists due to the lack of legislative enshrinement of this category. Electronic evidence is a much broader category and may include records stored, for example, by network or ISPs. Such data can be used in proof under a number of conditions. In addition, the evidence must always meet clear admissibility criteria. Appropriate legal regulation and specific legal regulations are needed to translate electronic information into electronic evidence. This largely explains why electronic proof is now at the stage of comprehension and theoretical substantiation. However, legal practice is

evolving and currently needs recommendations based on the generalization of positive experience with electronic means of proof.

The law defines a document as one of the types of procedural sources of evidence. The term "document" comes from the Latin word *documentum* and means "sample", "certificate", "proof". And in terms of etymological meaning of the term "document" philologists consider as:

- 1) business paper, certifying a certain legal fact, confirming the right to something, serves as proof of anything;
- 2) a written certificate officially confirming the identity;
- 3) written work, diploma, invoice, etc. as evidence of something historical, important;
- 4) special value - formatted paper data carrier, which is filled in automatically or manually [1].

The legal interpretation of the studied concept is broader, because in the foreground are the features that characterize its purpose, i.e. understand the materially fixed, reflected human message about legally significant facts.

According to the article of the Law of Ukraine "On Information", a document is a material medium containing information, the main functions of which are its saving and transmitting in time and space [2].

Electronic documents in terms of content determine numerous rights, constitutional and political issues, many of which have not yet been resolved. At the same time, the electronic document is important as evidence. The Criminal Procedure Code of Ukraine only defines a document as a source of evidence. corresponds to Part 1 of Art. 99 of the Criminal Procedure Code of Ukraine, a document is specially created for the use of information of a material object, which contains recorded by means of written signs, sound, images, etc., which can be used as evidence or is established during criminal proceedings. To the documents on the availability of information provided for in Part 1 of Art. 99 of the Criminal Procedure Code of Ukraine, may include photographs, sound recordings, video recordings and other media (including electronic).

An electronic document should be understood as "documented information presented in electronic form, thus an appendage for the reception of people using electronic computers, as well as for transmission over information and telecommunications networks or processing in information systems." Considering the two definitions in the system, we can draw the following conclusions:

-first, the concept of "document" (documented information) and "electronic document" are related by the legislator as a genus and species.

Secondly, the features of an electronic document are derived by indicating a special form of such a document - electronic.

In turn, the form of a document of legal literature is understood as its other features: the material on which it is made, as well as the way information is displayed. The specific form of the electronic document or, as scientists point out, the environment of its existence, determine the technological features of such documents, which are necessary with their help in various fields. These features are expressed in the following: first, the electronic document is not rigidly tied to the tangible medium - such a document is separated from it. Secondly, without compliance with certain conditions (especially the necessary hardware and software) such a document is difficult to accept people.

Third, it complicates the process of identifying an electronic document (such a document cannot be personally signed or identified without the use of appropriate software). Fourth, such a document is more accessible to a variety of changes.

Effective of the Criminal Procedure Code of Ukraine provides the opportunity to use e-mail, electronic information systems, electronic tools in the work of law enforcement and judicial authorities, but does not clearly define the electronic document. The only thing the legislator pointed out is that the original electronic document is its display, which is given the same meaning as the document (Part 3 of Article 99 of the Criminal Procedure Code of Ukraine) [3].

In Ukraine, the normative regulation of electronic evidence in criminal proceedings has only just begun with legislation, so there are problems with the practical application of this institution.

According to D. Tsekhan, when detecting digital information, investigators have significant difficulties in recording it, taking into account the requirements of criminal procedure law to evidence and further use in criminal proceedings. This is due to the ability to quickly change the content of the site, the physical location of servers in other countries, the use of anonymous packages, etc. [4]

Given that the term "electronic evidence" has already been introduced into legislation in other areas of law, as well as the fact that the Verkhovna Rada of Ukraine submitted a draft law "On Amendments to the Criminal Procedure Code of Ukraine to improve the fight against cybercrime and electronic evidence" № 4004 from 01.09.2020, which states that "electronic evidence is information in electronic (digital) form with information that can be used as evidence of a fact or circumstance established during criminal proceedings." [5], we are of the opinion that in order to unify the legal terminology it is expedient to use the term "electronic evidence".

At its core, electronic evidence is, first and foremost, a digital object that:

- was a means or instrument of committing a criminal offense (for example, a viral program through which unauthorized access to information was made; a telegram channel created for the sale of drugs, etc.);

- preserved electronic and digital traces of the criminal offense (for example, video from a digital video surveillance camera, which captures the image of the person who committed the criminal offense; metadata, which records the time of entry of an identified user into the automated system; information on electronic transfer of funds as an illegal benefit to an official, etc.);
- has been the subject of a criminal offense (for example, a website with pornographic material);
- was the object of criminally illegal actions (object of copyright, which was illegally distributed on the Internet; stolen cryptocurrency, etc.);
- contains other information that can be used as evidence of a fact or circumstance established during criminal proceedings (for example, information posted on a page on a social network allows to identify the accused).

According to Art. 84 of the Criminal Procedure Code of Ukraine evidence in criminal proceedings are 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 relevant to criminal proceedings and subject to proof.

Procedural sources of evidence are testimony, physical evidence, documents, expert opinions [6].

As for the concept of electronic evidence in criminal proceedings, according to N. Akhtyrskaya, "electronic evidence" is data that confirms facts, information or concept in a form suitable for processing by computer systems, including computer system programs or other actions. Sources of electronic evidence are electronic devices: computers, peripherals, computer networks, mobile phones, digital cameras and other portable devices, the Internet [7].

The introduction of the latest category of "electronic media" in the Criminal Procedure Code is due to the practical need to recognize these objects as a source of evidence in criminal proceedings. Literal interpretation of the text of Art. 99 of the Code of Criminal Procedure of Ukraine gives grounds to conclude that "electronic media" should be treated as any electronic media. Such media can be embedded in computer devices connected to the information network. They can contain materials in any form (written, graphic, photographic, video or audio, etc.). The legislator in Part 3 of Art. 99 of the Code of Criminal Procedure of Ukraine uses the term "electronic document", apparently, referring to the electronic media with the information recorded on it.

Criminal procedure legislation does not contain a definition of an electronic document. It is logical to assume that the term "electronic document" proposed in the Criminal Procedure Code of Ukraine should be interpreted as a kind, one of the forms of existence of another source of evidence - the document.

The document in its traditional meaning and the electronic document have a common feature - the information is stored and transmitted by describing events and facts using sign systems (texts, graphics, drawings, drawings, etc.) [8]. According to Art. 99 of the Criminal Procedure Code of Ukraine, a document is a material object specially created for the purpose of preserving information, which contains information recorded by means of written signs, sound, images, etc. that can be used by means of written signs, sound, images, etc. information that may be used as evidence of a fact or circumstance established during criminal proceedings.

In accordance with paragraph 1, part 2 of this article, the documents, provided they contain the information provided for in part 1 of this article, may include materials of photography, sound recording, video recording and other media (including electronic). In accordance with paragraph 3 of Part 2 of Art. 99 of the Code of Criminal Procedure of Ukraine, the documents may include media on which procedural actions are recorded by technical means, if they are compiled in the manner prescribed by the Code of Criminal Procedure of Ukraine.

In Part 3 of Art. 99 of the Code of Criminal Procedure of Ukraine states that the party to the criminal proceedings, the victim, a representative of the legal entity in respect of which the proceedings are conducted, are required to provide the court with the original document. The original of the document is the document itself, and the original of the electronic document is its display, which is given the same meaning as the document.

At its core, electronic evidence is, first and foremost, a digital object that:

- was a means or instrument of committing a criminal offense (for example, a viral program through which unauthorized access to information was made; a telegram channel created for the sale of drugs, etc.);
- Preserved electronic and digital traces of the criminal offense (for example, video from a digital video surveillance camera, which captures the image of the perpetrator; Metadata, which records the time of entry of an identified user into the automated system; Information on electronic transfer of funds provided as an illegal benefit to an official, etc.);
- has been the subject of a criminal offense (for example, a website with pornographic material);
- was the object of criminally illegal actions (object of copyright, which was illegally distributed on the Internet; stolen cryptocurrency, etc.);
- contains other information that can be used as evidence of a fact or circumstance established during criminal proceedings (for example, information posted on a page on a social network allows to identify the accused).

Electronic evidence has common features with traditional evidence, but at the same time has a number of unique characteristics:

- 1) they are not visible to the naked eye: sometimes they can be removed only by a specialist;
- 2) they are unstable, under certain circumstances the information in the device memory may be changed or lost. For example, if the device is depleted or there is not enough memory, the system imposes (writes) new information instead of the previous one, which means that the evidence can be destroyed. Computer memory can be damaged or destroyed by physical factors (high humidity, high temperature) and electromagnetic waves;
- 3) they can be copied without loss of quality an unlimited number of times, and any subsequent copy will not differ from the original [7];
- 4) can be both created by man and be the result of the functioning of the information system;
- 5) move freely in the electronic network without technical media and do not have an inseparable connection with the material media;
- 6) require a specific procedure for collection, inspection and evaluation [9].

Among the common features of electronic evidence, experts point out the following:

- exist in intangible form;
- can be created by man or be the result of functioning information system;
- cannot exist outside the technical medium or communication channel;
- do not have an inseparable connection with the material carrier;
- move freely in the electronic network without technical media;
- they can not be directly perceived and explored, only with help hardware and software;
- require a specific procedure for collection, inspection and evaluation;
- have the ability to dub, ie copy or move to another medium without loss of its characteristics;
- the possibility of remote modification and destruction [9].

Article 31 of the Constitution of Ukraine guarantees everyone the secrecy of correspondence, telephone conversations, telegraph and other correspondence. Exceptions may be established only by a court in cases provided by law, in order to prevent crime or to find out the truth during the investigation of a criminal case, if it is not possible to obtain information by other means [10].

The content of the electronic media is inspected not only in order to identify the files stored on it, but also in order to record the correspondence contained in SMS and other messages. In our opinion, there are debatable issues related to the review of information contained in the memory of phones, tablets, laptops, etc. without court permission. After all, such a review violates the constitutional rights of participants in criminal proceedings and others to the

secrecy of correspondence, telephone conversations, as the secrecy of communication is one of the general principles of criminal proceedings.

In accordance with paragraph 8 of Part 1 of Art. 1 of the Law "On protection of information in information and telecommunication systems" of July 5, 1994 № 80/94, information system is an organizational and technical system, which implements the technology of information processing using hardware and software. Thus, information systems include computers, mobile phones, tablets and other devices used to process information using software [11].

The mobile phone of any person contains personal correspondence with other citizens in SMS-messages, social networks, for example in "WhatsApp", "Telegram", "Viber", etc.

Norms of Criminal Procedure Legislation of Ukraine (Part 2 of Article 264 of the Code of Criminal Procedure of Ukraine) stipulate that it does not require the permission of the investigating judge to obtain information from electronic information systems or parts thereof, access to which is not restricted by its owner, owner or holder. associated with overcoming the system of logical protection [12-14].

Today, the issue of electronic evidence in criminal proceedings is of most interest to forensic scientists, while experts in the field of criminal proceedings undeservedly ignore this topic. In addition, the category of "electronic evidence" is part of the study of criminal procedural theory of evidence, and promising forensic doctrine of the collection, study and use of evidence in criminal proceedings. Legislative consolidation and implementation of this type of evidence requires doctrinal support from scientists - representatives of both these areas of knowledge.

Conclusions

Widespread introduction of information technology in all spheres of human life, dictated by advances in technological progress, leads to the gradual replacement of paperwork by electronic and entails the need to adapt legislation to the new conditions of the information society. Modern interpretation of the concept of "document", which takes into account the achievements of technical progress, allows to refer to documents of various types, including electronic documents, which determines the logical patterns of their use in all spheres of life, including legal. In this case, the common law concept of the document is specified within the conceptual apparatus of a particular industry. Despite the general functional purpose of traditional and electronic documents, electronic documents have some technological features that must be taken into account when using them in different legal relationships. Secondly,

without meeting certain conditions (availability of the necessary hardware and software) such a document is compiled for direct human perception. Third, the process of identifying the author of an electronic document is complicated (such a document cannot be personally signed or identified without the use of appropriate software). more accessible for a variety of changes. In order to determine the essence of the electronic document as evidence in criminal proceedings, it is necessary to focus on the requirements of criminal procedure law. Electronic documents as evidence in criminal proceedings are placed in the existing system of evidence and can be attributed either to other documents or to physical evidence. There is no reason to single out electronic documents as an independent type of evidence. Summarizing the above, it should be noted that the problem of doctrinal and legislative definition of electronic evidence is extremely relevant. After analyzing the opinions of scientists in this regard, we concluded that in essence, electronic evidence is a digital object that was a means or instrument of committing a criminal offense, preserved electronic and digital traces of a criminal offense, was the subject or object of a criminal offense or contains other information that can be used as evidence of a fact or circumstance established during criminal proceedings. In view of the above, we see an urgent need to formulate doctrinal and legal definitions of "electronic evidence" in criminal proceedings and in the scientific development of basic approaches to the collection, research and use of electronic evidence with further consolidation of such approaches in the Criminal Procedure Code of Ukraine.

References

- [1] Large explanatory dictionary of the modern Ukrainian language: 250 000 words / Uklad. and heads. ed. V.T. Stork. Kyiv; Irpen: Perun, 2005. VIII, 1728 p. URL: <http://irbis-nbuv.gov.ua/cgi-bin/ua/elib.exe? Z2IID = & I21DBN = UKRLIB & P21DB N = 1 & S21REF = 10 & S21FMT = online>
- [2] Law of Ukraine "On Information". Document 2657-XII, in force. Edited on 16.07.2020, basis -692-IX. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
- [3] Criminal Procedure Code of Ukraine: Law of Ukraine of April 13, 2012 № 4651-VI. Date of update: 04/24/2018. URL: <http://zakon0.rada.gov.ua/laws/show/4651-17>
- [4] Cehan D. Digital evidence: concepts, features and place in the system of evidence. Scientific Bulletin of the International Humanities University. 2013. №5. Pp. 256-259
- [5] Draft Law on Amendments to the Criminal Procedure Code of Ukraine to increase the effectiveness of the fight against cybercrime and the use of electronic evidence from 01.09.2020 № 4004. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771
- [6] Criminal Procedure Code of Ukraine: scientific and practical commentary / resp. ed. : SV Kivalov, SM Mishchenko, V. Yu. Zakharchenko. - H.: Odyssey, 2013. - 1104 p
- [7] Akhtyrskaya N. To the question of the probative force of cyberinformation in the aspect of international cooperation during criminal proceedings [Electronic resource] / N. M. Akhtyrskaya // Scientific Bulletin of Uzhhorod National University. - 2016. - Issue. 36 (2). - P. 123–125.
- [8] Sheremet A. Theoretical foundations of sources of evidence - Kyiv: Publishing House of Europe. University, 2012. - 110 s.
- [9] Alekseeva-Protstyuk D., Briskovskaya O. Electronic evidence in criminal proceedings: concepts, features and problematic aspects of application. Scientific Bulletin of Public and Private Law. 2018. Vip. 2. pp. 247–253
- [10] Constitution of Ukraine: as of January 1, 2020 URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
- [11] On information protection in information and telecommunication systems: Law Of Ukraine of July 5, 1994 № 80/94. URL <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
- [12] Criminal Procedure Code of Ukraine: Law of Ukraine of April 13, 2012 № 4651-VI. As of July 21, 2021. URL:<https://zakon.rada.gov.ua/laws/show/4651-17#Text>
- [13] Tetiana Kronivets, Yelyzaveta Tymoshenko, Oksana Diachenko, Tetiana Shabelnyk, Nadiia Ivanchenko, Svitlana Iasechko Artificial Intelligence as A Key Element of Digital Education / IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.106 pp. 67-72 <https://doi.org/10.22937/IJCSNS.2021.21.10.9>
- [14] Svitlana Iasechko, Alla Ivanovska, Tetyana Gudz, Mykola Marchuk, Oleksandr Venglinskyi, Alla Tokar Information as An Object of Legal Regulation in Ukraine/ IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.5, pp. 237-242 <https://doi.org/10.22937/IJCSNS.2021.21.5.33>