Advances in Social Science, Education and Humanities Research, volume 617
Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021)

Use of Electronic Evidence in Criminal Proceedings in Ukraine

Roman Blahuta [1] [0000-0002-8087-5995], Anatolii Movchan [1 *] [0000-0002-6997-6517], Maksym Movchan [2] [0000-0002-2099-3981]

[1] *Lviv State University of Internal Affairs, Lviv, Ukraine*
[2] *National Police of Ukraine, Kyiv, Ukraine*
[*] *movchan.anatol@gmail.com*

ABSTRACT
The article deals with the issues of documenting and using electronic evidence in criminal proceedings in Ukraine. The task of the study led to the use of dialectical, historical-legal, comparative-legal, system-structural, statistical and formal-logical methods. It is emphasized that the features of electronic (digital) evidence are that it is hidden (like fingerprints or DNA); easily crosses borders of jurisdiction; may be altered, damaged or destroyed; can be vulnerable, time sensitive. Signs and types of electronic evidence and basic principles of working with them are defined. The peculiarities of conducting operational and technical measures and unspoken investigative (investigative) actions with electronic evidence are analyzed: removal of information from transport telecommunication networks and removal of information from electronic information systems. Fixing of electronic evidence obtained as a result of investigative (investigative) actions or unspoken investigative (investigative) actions envisaged by the Criminal Procedure Code of Ukraine is carried out in compliance with certain requirements to the form and content. It is noted that forensic research is the main focus of documenting electronic evidence. It is emphasized that law enforcement officials should be properly trained in order to be able to effectively use electronic evidence in criminal proceedings, as well as to document the illegal activities of both individual offenders and organized criminal groups.

Keywords: *criminal proceedings, electronic digital signature, electronic evidence, e-mail, forensic research.*

1. INTRODUCTION

According to Art. 84 of the Criminal Procedure Code (CPC) of Ukraine, in criminal proceedings, evidence is "factual data obtained in the manner prescribed by this Code, based on which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subjected to proof" [1].

In 2017, a new chapter was introduced into the Code of Civil Procedure (CCP), Economic Procedural Code (EPC), Code of Administrative Procedure (CAP), which expanded the possibilities of the parties in the case – electronic evidence. Currently, some judicial practice of its use has already been accumulated in Ukraine [2].

At the same time, it should be noted that the CPC of Ukraine and the Code of Ukraine on Administrative Offenses have not received the institution of electronic evidence. This selective approach is not entirely clear and the following statements prove it. There is Chapter XVI "Criminal offences against computers, computer systems and networks" in the Criminal Code (CC) of Ukraine. There is also liability for illegal actions with electronic money (Art. 200 of the CC of Ukraine) or for fraud committed by unlawful operations, involving computerized equipment (Art. 190 of the CC of Ukraine).

Moreover, cybercrime has spread significantly [3]. In particular, according to the official data of the National Police of Ukraine, during 2020 more than 5,000 cybercrimes were registered in Ukraine, in which 106 participants of criminal proceedings, including 13 pedophiles, were promptly detained. In addition, the cyberpolice service received more than 100,000 calls and more than 40,000 electronic applications [4].

ISO/IEC 27037:2017 "Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence" entered into force on January 1, 2019, and digital evidence is defined as "information or data stored or transmitted in binary form that may be relied as evidence" [5, 6].

Electronic documents were recognized as evidence in the decisions of the European Court of Human Rights, in particular in the cases of "P. and S. v. Poland" (2012), "Eon v. Poland. France" (2013), "Shuman v. Poland" (2014) [7].

Some issues of using electronic evidence in criminal proceedings were considered in scientific works by Ukrainian scientists: Axtyrska N., Blaguta R., Chernyavskyj S., Gongalo S., Hutsaliuk M., Kalancha I., Kovalenko A., Khakhanovskyi V., Khyzhniak Ye., Kravchenko O., Makaruk K., Movchan A., Muradov V., Orlov Yu., Ratnova A., Sokolov M., Studennykov S., Stolitnij A., Tsekhan D. and other authors.

In particular, the leading areas of research are:

– the state of scientific development and normative regulation of the use of digital evidence in criminal proceedings [8];

– problematic issues of the use of electronic evidence in the criminal process of Ukraine [9-11];

– features of review of electronic documents during the investigation of criminal offenses [12].

Problematic issues of the use of electronic evidence in criminal proceedings have been the subject of research by foreign authors Kim H., Lee S., Mason S., Seng D. and others [13-17].

Despite the large number of publications on this topic, the problems of using electronic evidence in criminal proceedings in Ukraine remain insufficiently studied and require further research.

2. METHODOLOGY OF RESEARCH

The purpose of the study is to examine the use of electronic evidence in criminal proceedings in Ukraine. To achieve this goal, the task was set: to study the organizational and legal framework for documenting and using electronic evidence in criminal proceedings; to investigate the peculiarities of carrying out operational and technical measures and covert investigative (search) actions with electronic evidence.

The task of the study led to the use of dialectical, historical-legal, comparative-legal, system-structural, statistical and formal-logical methods.

3. RESULTS AND DISCUSSION

3.1. Organizational and legal bases of documentation and use of electronic evidence in criminal proceedings in Ukraine

Khakhanovskyi, V. & Hutsaliuk, M. suggest to consider the information in an electronic (digital) form obtained in the procedure provided by the CPC and matters to criminal proceedings as electronic evidence [8].

It is suggested in the Project of the Law "On Amendments to the Criminal Procedural Code of Ukraine to improve the effectiveness of combating cybercrime and use of electronic evidences" (Reg. No. 4004 dated 01.09.2020) to determine the electronic evidence as the information in electronic (digital) form with information that may be used as evidence of fact or circumstances established during criminal proceedings [18].

Features of electronic evidence are as follows: it is hidden (as fingerprints or DNA); it easily crosses the borders of jurisdiction; it can be changed, damaged or destroyed, it is vulnerable and time-sensitive.

Electronic evidence is characterized by the following features: impossibility of direct detection of a person at the physical level; unsteadiness; a change or destruction in the process of normal operation of the device; possibility of copying without loss of quality.

The types of electronic evidences are:

- local traces: traces of direct influence; evidences of indirect influence; distortion of information; destruction of information; information blocking; lack of access; violation of confidentiality; disruption of the computer;

– network traces: user data (contact details, address, phone, name, etc.); Message data (phone number, log files of access to one or another information systems);

– electronic information: digital photographs; video content; text documents; websites (pages); metadata; databases.

The original of electronic evidence is its reflection, which is given the same meaning as a procedural source of evidence. A copy of the electronic evidence, which is made by the investigator, the prosecutor with the involvement of a specialist, is recognized by a court as an original of electronic evidence.

For example, on February 14, 2019, the Grand Chamber of the Supreme Court, while reviewing the case № 9901/43/19 (P / 9901/43/19), decided that EDS is the main requisite of this form of electronic evidence. The absence of such requisite in the electronic document excludes grounds to consider it original, and therefore appropriate evidence in the case [20].

On September 10, 2019, the Supreme Court as a member of the panel of judges of the Administrative Court of Cassation in the case № 640/1374/19, administrative proceedings № K/9901/16734/19, K/9901/19224/19, K/9901/19231/19 (USSRU № 84134028) clearly stated that procedural documents received by the court using the service "Electronic Court" are considered to be submitted using their own electronic signature [20].

There is much debate about the need for EDS in the case of evidence of e-mail. However, in the Resolution of the Supreme Court of November 27, 2018, the panel of

judges noted that the conclusions of the courts on the inadequacy of printouts of electronic correspondence contradict the provisions of Art. 8 of the Law of Ukraine "On electronic documents and electronic document management", as the force of an electronic document as evidence can not be denied solely because it has an electronic form and is not further confirmed by the testimony of witnesses (correspondents) [21].

Sometimes the parties often refer to information from the opponent's social networks as evidence. As a rule, courts use such evidence. For example, negative statements on Twitter were the basis for the decision to refuse to recognize the plaintiff as a refugee or a person in need of additional protection [22].

Electronic evidence must be kept throughout the criminal proceedings. Upon the request of the holder of the electronic evidence an investigator, prosecutor, court may issue copies of this electronic evidence, if necessary – its original, attaching instead to the criminal proceedings copies certified by a qualified electronic signature of a judge, prosecutor or investigator.

The basic principles of handling electronic evidence are as follows:

1) it is necessary to ensure the integrity of the selected material and preserve the history of its transmission through continuous instrumental control during data retrieval;

2) any action taken on electronic evidence must be documented so that an independent third party can repeat the action and obtain a similar result;

3) a support of specialists is necessary who must have: special knowledge and experience in the relevant field; experience and skills in dealing with digital sources of information; understanding of the research question; necessary legal knowledge; appropriate communication skills (to enable them to give oral and written explanations); sufficient and necessary language skills; legal grounds for involvement in procedural actions;

4) if specialists in digital information sources are not present during the inspection, the officials conducting the investigative actions at the inspection or crime scene must have the necessary knowledge to identify and collect evidence;

5) authorities and officials conducting investigation are obliged to comply with the law, general forensic and procedural principles [23].

3.2. Features of operational and technical measures and covert investigative (search) actions with electronic evidence

Carrying out operational and technical measures and covert investigative (search) actions with electronic evidence is characterized by the following features:

1) inspectation of information from transport telecommunication networks – is to monitor and record the content of information by authorized operational units:

– by the address in the packet-switched data network (IP address on the Internet);

– by the hardware address of the device connected to the network environment (MAC address);

– by e-mail address;

2) inspectation of information from electronic information systems – is to identify and record the information contained in the electronic information system by:

– direct (physical) access;

– remote (software) penetration [23].

One of the software products that helps to get information about the owner of the domain (site), his/her IP address and find out where the server with the site (hosting or colocation) is located, there is the program IP-Tools.

In addition, there are free services on the Internet that can be used to get information about the resources of the network (sites) (SmartWhois, Mod IP City, etc.).

The Ping program that comes with Windows can be used to find the IP address of a site with a known domain name.

To obtain information about the traffic, the initiator sends the provider the decision of the investigating judge to withdraw information from technical communication channels, computer systems and other technical means, as well as a request on an official form with a stamp.

The provider independently prepares information about the connections made in accordance with the requirements of the request and sends a response to the initiator of the event.

Consolidation of electronic evidence obtained as a result of the investigative (search) actions or covert investigative (search) actions provided by the CPC of Ukraine is carried out in compliance with certain requirements for the form and content, in particular:

– procedural registration of protocols, involvement of a specialist, attesting witnesses, taking measures for the proper safety of digital data carriers;

– meaningful content of information, qualitative and quantitative components, completeness of the received information [23].

In some investigative actions, the participation of attesting witnesses is not obligatory, however, it gives more weight to the evidence obtained.

As part of the recording of electronic evidence, the investigator should be guided towards the use of data carriers that cannot be re-recorded.

We support the proposal to amend Art. 159 of the CPC of Ukraine on the introduction of temporary access to information in electronic (digital) form, things and documents, which consists in providing the party to the criminal proceedings by the person in possession of such information, things and documents, the opportunity to get acquainted with them, make copies of them and remove them (to seize them). In addition, it is proposed to regulate the special confiscation procedure of virtual assets. Today, special confiscation does not cover virtual assets, although the legalization (laundering) of proceeds from crime is carried out mainly through unregulated virtual markets [18].

We consider it expedient to submit for examination the question of the presence of signs of outside interference in electronic evidence, which is regulated by the relevant norms of the CPC of Ukraine:

• inspection, search, investigative experiment, etc. – within the framework of investigative actions in accordance with Art. 104 of the CPC of Ukraine – is accompanied by notes of attributes, indication of sources of origin of data and objects;

• within the framework of covert investigative (search) actions (in accordance with Articles 246-275 of the CPC of Ukraine);

• as a result of an expert forensic examination [23].

Forensic examination is the main direction of documenting electronic evidence. The forensic process is characterized by the following stages:

1) collection of information – accompanied by attribute notes, indications of data and objects sources;

2) examination by experts – involves reading it from the media carrier, decoding and extracting the necessary information relating to criminal proceedings;

3) analysis of information – to obtain answers to questions asked to an expert or specialist;

4) preparation of the conclusion – registration of results of examination and the analysis in the document established by the law and in the clear form [23].

Technical implementation of documentation and recording of electronic evidence can be carried out by: fixing the source code of the web page; video camera shooting; video capture screen.

To clarify the circumstances relevant to criminal proceedings, evidence in electronic form is provided to specialists to perform such types of forensic examinations as:

– engineering and technical (computer and technical, telecommunications);

– phototechnical, portrait and holographic images;

– video, sound recording;

– expertise in the field of intellectual property, etc. [24].

Issues that are resolved during these expert studies, directly or indirectly relate to the provision of the original or copy of electronic evidence for research, as indicated in the expert opinion.

When providing originals (or copies) of electronic evidence obtained during investigative actions for expert examination, the parties of the criminal proceedings encounter a problem such as a correct determination of the type of electronic evidence, namely, whether it is the original or a copy, because sometimes electronic evidence is copied on several media carriers for storage or further investigation of the circumstances of the case.

After the case file is submitted to the court, expert opinions based on copies of electronic evidence are often rejected by the judge if the electronic copies have not been certified by an electronic digital signature or their identity with the original has not been proved.

That is, there is a need to confirm the integrity and immutability of electronic information provided as evidence in criminal proceedings, in the case of its rewriting on various media carriers and transmission by electronic means. One way to confirm the integrity and immutability of electronic information during its storage, rewriting, transfer and transmission through communication channels is the calculation and verification of the checksum of files [9].

4. CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Law enforcement officers must be properly trained to be able to effectively use electronic evidence in criminal proceedings, as well as to document the illegal activities of both individual offenders and organized crime groups.

The basic principles of handling electronic evidence are as follows: it is necessary to ensure the integrity of the selected material and preserve the history of its transmission; any action taken on electronic evidence must be documented; a support of specialists is necessary who must have experience and skills in dealing with digital sources of information; authorities and officials conducting investigation are obliged to comply with the law, general forensic and procedural principles.

Carrying out operational and technical measures and covert investigative (search) actions with electronic evidence is characterized by the following features:

– inspectation of information from transport telecommunication networks is to monitor and record the content of information by authorized operational units: by the address in the packet-switched data network; by the hardware address of the device connected to the network environment; by e-mail address;

– inspectation of information from electronic information systems is to identify and record the information contained in the electronic information system by: direct (physical) access; remote (software) penetration.

In addition, problems of using electronic evidence in criminal proceedings in Ukraine require further coordination of domestic legislation to harmonize it with European and international standards.

It is necessary to accelerate the adaptation of DSTU ISO/IEC 27037:2017 "Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence" to the current legislation of Ukraine, as well as the implementation of the provisions of the Council of Europe Convention on Cybercrime on the mandatory storage and provision at the request of law enforcement agencies by telecommunications operators and providers of information necessary for the investigation of cybercrime.

We support the proposal to amend Art. 159 of the CPC of Ukraine on the introduction of temporary access to information in electronic (digital) form, things and documents. In addition, it is proposed to regulate the special confiscation procedure of virtual assets.

REFERENCES

[1] The Criminal Procedure Code of Ukraine, available at: https://zakon.rada.gov.ua/laws/main/ 4651-17

[2] Studennykov, S. (2019), "Electronic evidence in procedural law: how it works in Ukrainian realities", *Sudebno-yurydycheskaia hazeta*, 8 apr. 2019, available at: https://sud.ua/ru/news/publication/ 138354-elektronni-dokazi-v-protsesualnomu-pravi-yak-tse-pratsyuye-v-ukrayinskikh-realiyakh

[3] Kovalchuk, T.I. Korystin, O.Y. and Sviridyuk, N.P. (2019), "Hybrid threats in the civil security sector in Ukraine", Problems of Legality, vol. 147, pp. 163-175, DOI: 10.21564/2414-990x.147.180550

[4] Babanina, V. Tkachenko, I. Matiushenko, O. & Krutevych, M. (2021), "Cybercrime: History of formation, current state and ways of counteraction. Revista", *Amazonia Investiga*, vol. 10 (38), pp. 113–122. DOI: 10.34069/AI/2021.38.02

[5] DSTU ISO / IEC 27037: 2017 "Information technologies. Methods of protection. Guidelines for the identification, collection, acquisition and storage of digital evidence" (ISO / IEC 27037: 2012, IDT): Order of UkrNDNC dated 06.12.2017 № 400.

[6] Joseph Kithinji, Makau S. Mutua and Gitonga D. Mwathi (2021), "An Enhanced List Based Packet Classifier for Performance Isolation in Internet Protocol Storage Area Networks", *International Journal of Information Technology and Computer Science*, vol. 13, no. 5, pp. 51-63. DOI: 10.5815/ijitcs.2021.05.05

[7] Judgment of the European Court of Human Rights: Chamber judgment P. and SM. v. Poland, 30.10.12. Еон (EON) against FRANCE (Eon v. France): ECtHR decision / European Court of Human Rights judgments on the right to freedom of expression Bulletin XXXVII: Round-up of Judgements: June 2014 – 10 July 2014, available at: http://hudoc.echr.coe.int/fre-press?i=003-4140612-4882633);

[8] Khakhanovskyi, V. & Hutsaliuk, M. (2019), "The peculiarities of digital evidence use in criminal proceedings", *Forensic Bulletin*, no. 1 (31), pp. 13–19. DOI: 10.37025/1992-4437/ 2019-31-1-13

[9] Kravchenko, O. & Makaruk, K. (2019), "Problematic issues of application of technical means of fixation and their results in proving in criminal proceedings in the aspect of reforming criminal justice in Ukraine", *Bulletin of the Prosecutor's Office*, no. 6, pp. 67–76.

[10] Orlov, Yu. & Chernyavskyj, S. (2017), "Use of electronic mappings as evidence in criminal proceedings", *Scientific Bulletin of the National Academy of Internal Affairs*, no. 3 (104), pp. 13–24.

[11] Stolitnij, A. & Kalancha, I. (2019), Formation of the institute of "electronic evidence" in the criminal process of Ukraine", *Problems of Legality*, vol. 146, pp. 179–191.

[12] Khyzhniak, Ye. (2017), "Reculiarities of the digital document review during the investigation of criminal offenses", *State and Regions. Law Series*, no. 4 (58), pp. 80–85.

[13] Kim, H. & Lee, S. (2005), "Digital evidence collection process in integrity and memory information gathering". DOI: 10.1109/SADFE.2005.9

[14] Mason, S. (2016), "A Convention on Electronic Evidence: helping to provide for certainty in international trade". DOI: 10.14296/deeslr.v13i0.2321

[15] Mason, S. & Seng, D. (2017), "Electronic Evidence: Fourth Edition". DOI: 10.14296/517.9781911507079

[16] Erhan, Akbal and Sengul, Dogan (2018), "Forensics Image Acquisition Process of Digital Evidence", *International Journal of Computer Network and Information Security*, vol. 10, no. 5, pp. 1-8. DOI: 10.5815/ijcnis.2018.05.01

[17] Shuaibur Rahman and M. N. A. Khan (),"Digital Forensics through Application Behavior Analysis", International Journal of Modern Education and Computer Science(IJMECS), Vol.8, No.6, pp.50-56, 2016.DOI: 10.5815/ijmecs.2016.06.07

[18] Monastyrsky, D. & etc. (2020), On Amendments to the Criminal Procedure Code of Ukraine to Increase the Effectiveness of the Fight against Cybercrime and the Use of Electronic Evidence: Draft Law (Reg. № 4004 of 01.09.2020), available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

[19] Order of 02/14/2019, No. 9901/43/19: Supreme Court. Grand Chamber, available at: https://verdictum.ligazakon.net/document/79883385

[20] Order of the Supreme Court within the Board of Judges of the Administrative Court of Cassation in Case No. 640/1374/19 of 10 September 2019, Administrative Procedure No. K / 9901/16734/19, K / 9901/19224/19, K / 9901/19231 / 19 on the claim to the Deposit Guarantee Fund of individuals for recognition of illegal actions and obligation to take actions, available at: http://reyestr.court.gov.ua/Review/84134028

[21] Electronic Evidence in Court Practice, available at: https://sud.ua/ru/news/publication/138970-elektronni-dokazi-v-sudoviy-praktitsi

[22] Resolution of the Sixth Administrative Court of Appeal of Kyiv on administrative case No. 826/18174/16 of March 19, 2019 against the appeal of the State Migration Service of Ukraine against the decision of the District Administrative Court of Kyiv of October 31, 2018 in the case of an administrative claim by a citizen of Ro The State Migration Service of Ukraine on the recognition of illegal and cancellation of the decision, the obligation to take action, available at: http://reyestr.court.gov.ua/Review/80579207

[23] Blaguta, R. & Movchan, A. (2020), *The latest technologies in crime investigation: current status and problems of use*, monograph, Lviv State University of Internal Affairs, Lviv, Ukraine.

[24] Klymchuk, M. Marko, S. Priakhin, Ye. Stetsyk, B. & Khytra, A. (2021), “Evaluation of forensic computer and technical expertise in criminal proceedings”, *Revista Amazonia Investiga*, vol. 10 (38), pp. 204–211. DOI: 10.34069/AI/2021.38.02.20