PROBLEMATIC ISSUES OF USING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS (SDG’S)

Tetiana Slipeniuk¹
Mykola Yankovyi ²
Viktor Nikitenko ³
Oleksandr Manzhai ⁴
Yuliia Tiuria ⁵

ABSTRACT

Objective: The object of this scientific publication is the use of electronic evidence in criminal proceedings, focusing on the main problematic issues, legislative gaps, and the need for improvements in law enforcement practices.

Method: The method of study involves a detailed analysis of the current criminal procedure legislation, identification of the general and special features of electronic evidence, and examination of practical issues related to the collection, assessment, and admissibility of electronic evidence in criminal proceedings. The authors use legal analysis and case studies to propose amendments to the legislation and suggest practical improvements.

Results: In this scientific publication, the authors highlight the main problematic issues of using electronic evidence in criminal proceedings, propose amendments to the current criminal procedure legislation, and also make proposals for improving law enforcement practice. It is argued that electronic evidence is an independent procedural source of evidence which has both general and special features and nowadays plays an important role in establishing the truth in criminal proceedings. It is concluded that the use of electronic evidence in criminal proceedings currently has no regulatory basis, which causes numerous difficulties and gaps which, among other things, lead to abuse of procedural powers.

Contribution: It is established that in the process of collecting electronic evidence, there are many abuses of procedural powers, which are expressed in the excessive seizure of their carriers, as well as unlawful interference with privacy. The article also reveals the difficulties in assessing electronic evidence as relevant, admissible and reliable evidence. In particular, the use of different copies of electronic documents, compliance by judges with the principle of direct examination of evidence, and the admissibility of electronic evidence obtained from open sources are controversial. Based on the results of the study, the authors propose to amend the Code of Criminal Procedure of Ukraine by supplementing Chapter 4 ‘Evidence and Proof’ with paragraph 5 ‘Electronic Evidence’, which should define their concept, procedural procedure for their seizure, storage, return, and peculiarities of evaluation. The authors also emphasises the expediency of upgrading the qualifications of authorised persons by conducting thematic training on the proper use of electronic evidence and preventing abuse of procedural powers in this process.

¹ National University “Odesa Law Academy”, Odesa, Ukraine.
E-mail: slipeniuk@gmail.com
² Odessa State University of Internal Affairs, Odesa, Ukraine.
E-mail: m802@ukr.net
³ State University of Trade and Economics, Kiev, Ukraine.
E-mail: viknik241@ukr.net
⁴ Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.
E-mail: sofst@ukr.net
⁵ Dnipro University of Technology, Dnipro, Ukraine.
E-mail: ivzhenkoss@gmail.com
Keywords: information, electronic evidence, criminal procedure, abuse of procedural powers, collection of evidence, evaluation of evidence, artificial intelligence, digital technology, civil and commercial procedure, sustainable development goals (SDG’s).

1 INTRODUCTION

The 21st century is rightly called the age of information technology. Digital technologies continue to evolve, and a large percentage of sectors of social life are developing along with them. The coronavirus pandemic of 2019 also significantly affected the scale and speed of digital transformation in many sectors, and even afterwards, the introduction of the latest technologies will always remain the main driver of growth for many organisations and a source of stable operations in emergency conditions, including war.

Digital technologies have changed the way we live our lives, improving them and providing access to unprecedented opportunities in human history. Unfortunately, however, progress and innovation are not only used for good, but have also become a tool for criminal activity. A fairly high percentage of modern criminal offences are committed with the help of information technology, so electronic evidence now plays a significant role in the evidence base in criminal proceedings.

Information that is essential for achieving the objectives of criminal proceedings may be contained in photo, video, sound recordings and electronic documents, as well as in data sets containing information on the operation of registers, databases, telecommunication networks, etc. The collection, verification and evaluation of the latter during criminal proceedings is gaining momentum, especially in the process of investigating criminal offences, in particular, military offences and offences against the foundations of national security.
2 THEORETICAL FRAMEWORK

At the same time, criminal procedure legislation has gaps and contradictions in the use of electronic evidence, which leads not only to difficulties in practice, but also to abuse of procedural powers.

Analysis of recent research and publications. The use of electronic evidence in criminal proceedings has already been in the field of view and has become the subject of scientific interests of such researchers as D. Alekseeva-Protsiuk, A. Angeleniuk, R. Blahuta, Briskovska O.M., Garasymiv O.I., Kovalenko A.V., Marko S.I., Meteliev O.P., Movchan A.V., Muzychenko O.V., Orlov Y.Y., Rachynskyi O.O., Ryashko O.V., Smal I.A., Skrypnyk A.V., Tsekhan D.M., Cherniavskyi S.S., Fomina T.G. and others. Despite the fact that the scientific achievements of the aforementioned authors have led to a significant scientific development of the doctrine, there are still certain aspects in this area which have no clear answers and which are problematic in practice. This necessitates a deep theoretical study of the issues related to the use of electronic evidence in criminal proceedings, as well as the formation of the author's own vision on the issue of improving the relevant regulatory framework and enhancing the efficiency of criminal proceedings.

3 METHODOLOGY

The purpose of this research is to comprehensively study the main problematic issues of the use of electronic evidence in criminal proceedings, and also to provide arguments and formulate the author's own scientific conclusions regarding possible changes to the current criminal procedure legislation and improvement of law enforcement practice. The outlined purpose of the study necessitated disclosure of the provisions of legal acts and court decisions of various instances, as well as scientific publications of foreign and domestic researchers.

To achieve the research objectives, the following methods were used:
The dialectical method: provided for consideration of the use of electronic evidence in dynamics and development, allowing to identify the main trends and problems of their use in modern criminal proceedings.

Methods of analysis and synthesis: used for a detailed study of certain aspects of the problem and generalisation of the results obtained, which contributed to the formulation of holistic scientific conclusions.

Systemic and structural methods: allowed us to consider electronic evidence as an element of the criminal justice system, determine its place and role in procedural activities, and establish the relationship with other elements of the system.

The statistical method was used to analyse quantitative data on the use of electronic evidence in criminal cases, which allowed us to identify patterns and trends in their use.

Formal and logical method: ensured clarity and consistency of presentation of the material, contributed to the logical justification of scientific conclusions and proposals.

The dogmatic method: used to analyse current legislation and law enforcement practice, which allowed us to identify gaps and shortcomings in the legal regulation of the use of electronic evidence.

Hermeneutic method: allowed for a deeper understanding of the content of legal provisions governing the use of electronic evidence and their interpretation in court practice.

The use of an integrated approach and various research methods ensured a comprehensive study of the issues related to the use of electronic evidence in criminal proceedings, which allowed the author to formulate sound scientific conclusions and proposals for improving legislation and practice of their application.

4 RESULTS AND DISCUSSION

Scientific and technological progress, global informatisation of modern society and the widespread use of electronic means of communication are leading to a qualitatively new level of legal proceedings. Thus, the Law of
Ukraine ‘On Amendments to the Commercial Procedure Code of Ukraine, the Civil Procedure Code of Ukraine, the Code of Administrative Procedure of Ukraine and Other Legislative Acts’ of 03.10.2017 No. 2147-VIII introduced revolutionary changes to the Commercial Procedure Code of Ukraine, the Civil Procedure Code of Ukraine and the Code of Administrative Procedure of Ukraine, which introduced the e-justice system at all stages of civil, commercial and administrative proceedings. The latter is designed to ensure that justice is administered in real time and is as simple and accessible as possible. In addition, this regulatory legal act enshrines a relatively new category in domestic legislation - ‘electronic evidence’.

Analysis of the provisions of Article 96 of the Commercial Procedural Code of Ukraine, Article 100 of the Civil Procedural Code of Ukraine and Article 99 of the Code of Administrative Procedure of Ukraine indicates that the legislator interprets the category of ‘electronic evidence’ as ‘information in electronic (digital) form containing data on circumstances relevant to the case, in particular, electronic documents (including text documents, graphic images, plans, photographs, video and sound recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases and other data in electronic form’.

However, these progressive changes have not been introduced to the Criminal Procedure Code of Ukraine. Thus, part 2 of Article 84 of the Criminal Procedure Code of Ukraine defines the system of procedural sources of evidence as a set of testimonies, material evidence, documents, and expert opinions. Despite the fact that electronic evidence is not endowed with the status of procedural sources of evidence, the latter are increasingly becoming the object of practical activity of authorised persons, as the number of criminal offences with digital traces (photos, videos, network connection traffic, etc.) is constantly growing, which is especially relevant in the context of investigating crimes committed by the Russian occupiers.

The needs of practice have led to scientific discussions on the content and peculiarities of using electronic evidence in criminal proceedings.

Thus, there is currently a lively debate about the name of this procedural source of evidence. The prevailing opinion is the term ‘electronic evidence’, 
which is shared by the majority of the scientific community. Thus, D.O. Alekseeva-Protsyuk and O.M. Briskovska believe that ‘electronic evidence is factual data stored in electronic form on any type of electronic media and in electronic means and which, after processing by special hardware and software, become available for human perception’ (ALEKSEEVA-PROTSIUK D.O., BRISKOVSKA O.M., 2018). Some scholars believe that electronic evidence is evidence in criminal proceedings that can be obtained in electronic form (HUTSALIUK MV., HAVLOVSKYI V.D., KHAKHANOVSKYI V.H., 2020).

Another group of scholars defines this category as ‘digital evidence’. In particular, according to D.M. Tsekhan, ‘digital evidence’ should be understood as ‘factual data presented in digital (discrete) form and recorded on any type of media and, after processing by a computer, become available for human perception. At the same time, a mandatory feature of digital evidence is convergence, which means the ability of a single piece of evidence to be included in a set of other evidence and acquire evidentiary value in this regard’ (TSEKHAN D.M., 2013).

The views of scholars who define the category under study as ‘electronic documents’ and ‘electronic displays’ are also of interest. For example, A.V. Ratnova defines ‘electronic documents’ as ‘information in electronic form that can be used as evidence of a fact or circumstances established in criminal proceedings’ (RATNOVA A.V., 2021). S.S. Chervniavskyi and Y.Y. Orlov understand ‘electronic displays’ as ‘any electronic media, in particular those built into computer devices connected to the information network. Such media may contain materials in any form (written, graphic, photographic, video, sound recording, etc.) (ORLOV Y.Y., CHERNIAVSKYI S.S., 2017).

There are also alternative views. In particular, A.V. Kovalenko notes that ‘neither the name “digital” nor the name “electronic” is optimal from a technical point of view. After all, there are now coding systems that are not based on the use of numbers, and computing devices and modern means of information transmission that do not use the movement of electrons (quantum computers, data transmission using optical signals, etc.). It is also predicted that with the development of science, other technologies will appear that, in
fact, will not correspond to the terms under consideration’ (KOVALENKO A.V., 2018).

In our opinion, the above names of this term are equivalent, since they carry the same semantic load: they are a set of factual data obtained in the manner prescribed by the CPC of Ukraine with the help of electronic devices, computer storage media, as well as computer networks, including the Internet, which are relevant for the performance of tasks assigned to criminal proceedings. Therefore, we believe that the discussion regarding the name of a new procedural source of evidence in the CPC of Ukraine should be resolved by the legislator by enshrining such a category in the CPC of Ukraine in compliance with the established legislative technique.

Analysing the scientific literature and legislation, it can be stated that electronic evidence has a number of properties which should be divided into two groups: a) general features of evidence inherent in all means of proof; b) special features of electronic evidence inherent only in this type of evidence (RIBEIRO, J., & GABRIEL, 2024). The general features include the features that are clearly enshrined in the CPC of Ukraine, namely: relevance (must contain information about the subject matter of proof), admissibility (must be obtained without violating the procedure established by law), reliability (allows to establish the actual circumstances of the criminal offence) and sufficiency (the totality of electronic evidence allows to summarise the presence/absence of circumstances that are part of the subject matter of proof).

While the general properties of evidence, including electronic evidence, are well-established in criminal procedural science, the specific properties are still under discussion. A study of the relevant scientific achievements in this area makes it possible to identify the most common views on the specific properties of electronic evidence in criminal procedure. These include: creation and display with the help of special technical means in an intangible form, repeated reproduction and copying without changing the essential characteristics, the possibility of transformation into other procedural forms of evidence, indefinite storage, combination of different forms of information, etc.
The versatility of electronic evidence and its importance for establishing the truth in criminal proceedings is increasingly raising the issue of its collection and evaluation by authorised entities in the absence of relevant provisions in the CPC of Ukraine.

The collection of electronic evidence during criminal proceedings is carried out by the parties thereto, as well as by the victim, a representative of the legal entity in respect of which the proceedings are being conducted, in accordance with the procedure established by the CPC of Ukraine.

The provisions of Article 93 of the CPC of Ukraine define different ways of collecting the evidence under investigation. However, the nature of electronic evidence implies the predominant use of public (search, inspection) and covert (audio, video monitoring of a person/place, removal of information from electronic communication networks/electronic information systems, monitoring of bank accounts, surveillance of a person, thing or place) investigative search actions to collect the latter (CORNEAU, 2023).

The analysis of domestic law enforcement practice shows that in order to establish the truth in the vast majority of criminal proceedings, searches are conducted, during which electronic evidence and their media may be seized. According to the provisions of Article 234 of the CPC of Ukraine, searches are conducted only on the basis of a decision of the investigating judge, which determines the list of things and documents to be seized. For example, by the decision of the Dzerzhynskiy District Court of Kryvyi Rih of 13.03.2023 in case 210/3565/22, in order to establish all the circumstances of the criminal offences under Part 4 of Article 190, Part 1 of Article 255 of the Criminal Code of Ukraine, the investigating judge ‘granted permission to seize computer equipment used in the seizure of funds, electronic databases on victims contained therein, network equipment, software used to make calls by victims, other software used to seize victims’ funds, other computer office equipment, servers containing traces of a criminal offence, in particular: system units of personal computers, laptops, tablets, mobile phones mobile phones of participants in criminal proceedings, SIM cards that served as means of communication during the commission of a criminal offence or other electronic
means of information transmission that may contain data on the organisation and commission of the said criminal offence’.

Despite the fact that this ruling is quite detailed, it contains a discretionary element - ‘other electronic means of information transmission’ - which leads to abuse of procedural powers. In particular, it is not uncommon for authorised persons, using their discretion, to unreasonably seize electronic evidence and computer equipment, servers, external storage media, mobile phones that are not carriers of such evidence, citing the need for computer and technical expertise, possible belonging to things obtained by criminal means, etc. An example of such an abuse can be seen in the decision of the Shevchenkovskyi District Court of Kyiv of 26.07.2019 in case No. 761/25264/19, which denied the seizure of seized items that, in the opinion of the prosecution, could be a source of electronic evidence.

The procedural mechanism for counteracting these abuses is judicial control, during which the investigating judge checks the validity of the temporarily seized property, considers complaints about the inaction of authorised entities regarding the failure to return the property in case of failure to file a motion for seizure no later than the next business day after the seizure, as well as the possibility of lifting the seizure. In addition, the CPC of Ukraine provides for the possibility of appealing the relevant rulings of the investigating judge on appeal.

When describing the problematic issues of using electronic evidence collected as a result of covert investigative (detective) actions, it is worth noting the unrestricted access of authorised persons to private information, which violates Article 32 of the Constitution of Ukraine and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and leads to abuse of procedural powers.

The procedural nature of covert investigative (detective) actions involves the collection of a large amount of information, which, among other things, includes confidential information that is not relevant to criminal proceedings, but their use may be interpreted as an intrusion into the subjective interests of a person. An example of such an intrusion is reflected in the decision of the Halytskyi District Court of Lviv dated 28.06.2023 No.
461/673/18, by which the court declared inadmissible electronic evidence obtained as a result of audio monitoring of a person, as it contains a recording of the accused’s conversations with the defence counsel.

The criterion for establishing the good faith of the use of procedural powers when dealing with electronic evidence containing private information obtained covertly is the need for such intervention in a democratic society to achieve a legitimate goal.

The European Court of Human Rights in the case of Klass and Others v. Germany of 06.09.1978 concluded that ‘secret surveillance of citizens, characteristic of a police state, may be permissible under the Convention for the Protection of Human Rights and Fundamental Freedoms only if it is strictly necessary for the functioning of democratic institutions. Thus, democratic societies are currently under threat from very sophisticated forms of espionage and terrorism, and as a result, the state must be able to effectively counter such threats and conduct covert surveillance of subversive elements operating on its territory. The Court considers that the existence of legislation giving legitimacy to the secret surveillance of electronic mail, post and telecommunications is, in exceptional circumstances, necessary to ensure national interests and security and/or to prevent disorder or crime.’

Sharing the opinion of the ECHR, the Criminal Court of Cassation of the Supreme Court in its decision of 21.03.2018 in case No. 751/7177/14 emphasises the expediency of applying another criterion: ‘the availability of adequate and sufficient guarantees against abuse, in particular, a clear and predictable procedure for authorisation, implementation of relevant operational and investigative measures and control over them’.

An important mechanism for preventing abuse of procedural powers and violation of the right to private information is also the prohibition of using information obtained as a result of such actions in another criminal proceeding. According to Article 257 of the CPC of Ukraine, the only exception is the permission of the investigating judge and confirmation of the fact that the prosecutor personally transmitted such information.

In the process of using electronic evidence, the issues related to their assessment as proper, admissible and reliable evidence are quite controversial.
As already noted, the CPC of Ukraine, unlike other procedural legal acts, does not contain any provisions on the procedure for seizure and proper storage of electronic evidence. This prevents the identification of the person who created the electronic evidence, creates the possibility of its modification or destruction, makes it difficult to reproduce in the original, as there are no official requirements for its form, and creates other difficulties and abuses.

In view of the above, defence counsels are increasingly filing motions to declare electronic evidence inadmissible (because the information was first copied to a computer and then to an optical disc, which was submitted to the court as a procedural medium of evidence), which has formed the relevant case law. In the decision of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court of 29.03.2021 in case No. 554/5090/16-κ, it was concluded that ‘the identification of electronic evidence as a means of proof and a material carrier of such a document is groundless, since a characteristic feature of an electronic document is the absence of a strict link to a specific material carrier. The same electronic document may exist on different carriers. All copies of an electronic document identical in content may be considered as originals and differ from each other only in time and date of creation. The issue of identifying an electronic document as an original may be resolved by the authorised person who created it (using special software to calculate the checksum of a file or a directory with files - CRC-sum, hash-sum), or, if there are appropriate grounds, by conducting special studies’.

A controversial issue in the process of studying the assessment of electronic evidence is the issue of compliance by judges with the principle of direct examination of evidence. According to Article 23 of the CPC of Ukraine, ‘the court examines evidence directly, and information contained in testimony, things and documents that have not been the subject of direct examination by the court cannot be recognised as evidence, except in cases provided for by this Code’. At the same time, during the trial, sometimes the court is unable to directly examine electronic evidence, since the relevant link on the Internet does not yield results or the link already contains other information. Therefore, the judges of the Supreme Court rightly raise the question of whether the study
of recorded and archived data as originals of digital information complies with the principle of direct examination of evidence.

We cannot ignore the issue of assessing the admissibility of electronic evidence obtained from open sources. The invasion of the territory of Ukraine by the Russian Federation has resulted in a number of criminal offences against the foundations of national security, as well as war crimes. Due to the circumstances of their commission, quite often the only evidence that allows establishing the truth in criminal proceedings is electronic evidence obtained from open sources. In the context of the issue raised, we consider it appropriate to draw attention to the E CtHR judgment in the case of Georgia v. Russia (II) of 21.01.2021, in which the Court referred to a report published by the American Association for the Advancement of Science (AAAS), ‘High-quality satellite imagery and the conflict in South Ossetia’ on 09.10.2008, and used the analysis of satellite imagery as electronic evidence.

5 FINAL CONSIDERATIONS

Based on the foregoing, it can be argued that currently the rules for the use of electronic evidence in criminal proceedings do not have a proper regulatory framework and are actually shaped by judicial practice. Many problematic and controversial issues can be resolved by amending the Criminal Procedure Code of Ukraine by supplementing Chapter 4 ‘Evidence and Proof’ with paragraph 5 ‘Electronic Evidence’, which defines their concept, procedural procedure for seizure, storage, return and specifics of evaluation. In addition, in our opinion, it is advisable to improve the qualifications of authorised persons by conducting thematic trainings on the proper use of electronic evidence and preventing abuse of procedural powers in this process.

Thus, the effective use of electronic evidence is an important element of modern criminal procedure that requires clear regulatory regulation. The absence of legislative regulation not only complicates the work with this evidence, but also creates opportunities for abuse and violations of the rights of participants in the process. The introduction of appropriate amendments to the Criminal Procedure Code of Ukraine regulating the use of electronic
evidence is a necessary step to increase the transparency and objectivity of criminal proceedings.

At the same time, it is important to ensure that law enforcement officers and judges are properly trained. Specialised trainings and educational programmes will improve their skills and ensure a professional approach to working with electronic evidence. This will contribute not only to a more efficient use of such evidence, but also to the prevention of possible abuses and errors in the procedural activities.

Summing up the results of the study, we conclude that, despite the lack of legislative consolidation, electronic evidence has long been a full-fledged procedural source of evidence, which sometimes plays a key role in establishing the truth in criminal proceedings. Today, the process of their use is accompanied by numerous difficulties and gaps, which, among other things, lead to abuse of procedural powers. Therefore, we hope that in the near future the Criminal Procedure Code of Ukraine will be supplemented with relevant provisions that will help to increase the efficiency of the use of electronic evidence in criminal proceedings. This will ensure a more objective and fair consideration of criminal cases, strengthen confidence in the judicial system and improve the quality of justice in Ukraine.
REFERENCES


Resolution of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court of 29.03.2021 in case No. 554/5090/16-к. URL: https://reyestr.court.gov.ua/Review/96074938


Judgment of the European Court of Human Rights in the case of Georgia v. Russia (II) of 21.01.2021. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%222001-207757%22]}

Judgment of the European Court of Human Rights in the case of Klass and Others v. Germany of 06.09.1978. URL: https://hudoc.echr.coe.int/eng#{i=001-57510}.

Supreme Court judges discussed with experts the admissibility of electronic evidence obtained from open sources. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/ 


Ruling of the Dzerzhynskyi District Court of Kryvyi Rih of 13.03.2023 in case 210/3565/22. URL: https://reyestr.court.gov.ua/Review/109662604


