УДК 343.14
DOI https://doi.org/10.24144/2307-3322.2023.80.2.28

E-EVIDENCE IN UKRAINIAN CRIMINAL JUSTICE: EXPLORING THE LEGAL REALITIES AND THEORETICAL PERSPECTIVES[1]

Nazarko A.,
PhD Research Fellow and MSCA4Ukraine Fellow
Faculty of Law at the University of Bergen
ORCID: https://orcid.org/0000-0002-4190-7288
e-mail: artem.nazarko@uib.no

Nazarko A. E-Evidence in Ukrainian Criminal Justice: Exploring the Legal Realities and Theoretical Perspectives.

This article delves into the intricate domain of electronic evidence (e-evidence) within the Ukrainian criminal justice system. The primary objective is to comprehensively dissect the multifaceted legal intricacies surrounding e-evidence, including its position and significance in Ukraine's ongoing quest for European integration and its response to the persistent armed conflict.

The article extensively examines the intricate complexities of e-evidence, exploring its pivotal role within the broader framework of procedural sources of evidence. It also scrutinises its interaction with traditional forms of evidence, shedding light on the evolving landscape of legal practices in a digital age. The article emphasises the urgent imperative for substantial enhancements in Ukraine's legal framework governing e-evidence. The existing framework falls short of contemporary standards, posing substantial impediments to effective law enforcement and judicial prosecution in this era of rapid technological advancements. To ensure accountability for past transgressions and to sustain the principles of the rule of law during the post-war era, Ukraine must harmonise its legal system with modern approaches to handling e-evidence.

In summary, this article offers a comprehensive and insightful analysis of the intricacies surrounding electronic evidence in the Ukrainian criminal justice system. It addresses critical legal dimensions, acknowledging their importance as Ukraine navigates a path towards integration with European legal standards and grapples with the ramifications of a prolonged armed conflict. The exploration presented here is a significant step towards a more profound understanding of the role and challenges of electronic evidence in the contemporary legal landscape.

Key words: criminal procedure law, electronic evidence, digital evidence, justice, accountability, Ukraine.

Назарко А.А. Електронні докази в українському кримінальному судочинстві: Дослідження правових реалій та теоретичних перспектив.

Ця стаття розглядає важливий аспект українського кримінального правосуддя – використання електронних доказів. Метою дослідження є аналіз правових складнощів, пов'язаних із цією темою, визначення місця електронних доказів у кримінальному судочинстві України та їх значення в контексті прагнення України до європейської інтеграції та подолання впливу триваючого збройного конфлікту.

Стаття висвітлює складнощі, пов'язані із використанням е-доказів, і досліджує їхню роль у загальному контексті процесуальних джерел доказів та їхню взаємодію з традиційними формами доказів. В статті також наголошується на тому, як електронні докази впливають на кримінальне судочинство в епоху цифрових технологій та в умовах триваючого конфлікту. Стаття аналізує

[1] This article relates to research that has received funding through the MSCA4Ukraine project (Project ID 1233453). The project is funded by the European Union. Views and opinions expressed are, however, those of the author only and do not necessarily reflect those of the European Union. Neither the European Union nor the MSCA4Ukraine Consortium as a whole nor the Alexander von Humboldt Foundation can be held responsible for them.

поняття електронних доказів та їх роль у сучасному цифровому суспільстві. Вона досліджує взаємодію електронних доказів з іншими видами доказів у контексті кримінального судочинства, а також визначає виклики, які виникають у зв'язку із збором, збереженням та використанням електронних доказів у судових процедурах. Дослідження акцентує увагу на необхідності вдосконалення законодавчого підґрунтя, що регулює питання використання електронних доказів в Україні. Поточний правовий база відстає від сучасних стандартів, що ускладнює ефективність правопорушення та судового переслідування в епоху цифрових технологій. Для забезпечення відповідальності за минулі злочини та зміцнення верховенства права, Україна має привести свою правову систему у відповідність із сучасними підходами до використання електронних доказів.

Автор підкреслює актуальність питання та необхідність внесення суттєвих змін у законодавство для відповідності сучасним підходам до електронних доказів. Це важливий крок для забезпечення відповідальності за минулі правопорушення та зміцнення верховенства права в постконфліктному періоді в Україні.

Ключові слова: кримінальне процесуальне право, електронні докази, цифрові докази, правосуддя, джерела доказів, кримінальне провадження.

1. Introduction

The category of electronic evidence (e-evidence) within the Ukrainian criminal justice system is a highly intricate and contentious domain, marked by unresolved questions and legal dilemmas. It navigates the uncharted waters of the digital age, presenting unique opportunities and formidable challenges for adjudicating criminal cases.

The rapid technological advancements and the evolving nature of digital communication further compound the use of e-evidence in the Ukrainian legal system. As these technologies continue to progress, it becomes imperative for the Ukrainian legal framework to adapt and stay abreast of the latest developments to effectively handle e-evidence. This entails understanding the technical aspects of data collection and preservation and the legal standards and procedures that align with international best practices.

The complexity of e-evidence in Ukrainian criminal law is underscored by its significance in the context of Ukraine's aspiration to integrate with the European Union, a pursuit that necessitates harmonising the Ukrainian legal framework with the European one. As Ukraine seeks to assert its commitment to the rule of law, justice, and accountability, understanding the complexities of e-evidence becomes pivotal.

This issue gains particular relevance against the backdrop of Russia's ongoing military aggression against Ukraine, which a multitude of documented war crimes has accompanied. From 24 February 2022, which marked the start of the large-scale armed attack by the Russian Federation, to 10 September 2023, the Office of the UN High Commissioner for Human Rights (OHCHR) recorded 27,149 civilian casualties in Ukraine: 9,614 killed and 17,535 injured [1]. Recent statistics of the Office of the Prosecutor General of Ukraine indicate an alarming tally of over 108,000 registered war crime cases since 24 February 2022 [2]. In response to the evolving landscape of armed conflict, numerous digital platforms and services have emerged, dedicated to collecting and preserving e-evidence related to war crimes. Examples include websites WarCrime.gov.ua, Dokaz.gov.ua, 5am.in.ua, Shtab.net, eyeWitness app, and others [3, 4, 5, 6, 7]. These platforms have introduced a novel dimension to the legal arena, raising intriguing questions about the admissibility, reliability, and treatment of e-evidence obtained through these services within the Ukrainian legal framework.

The article aims to reveal the essence and legal nature of the concept of e-evidence in the criminal procedure legislation of Ukraine. It analyses the place of e-evidence in the system of procedural sources of evidence and its correlation with other types of evidence. The article also explores possible ways of resolving the issue of the interpretation of e-evidence in the criminal legislation of Ukraine.

2. Legal Foundations and Theoretical Dimensions of E-evidence in Ukrainian Criminal Procedure Law

E-evidence in Ukrainian criminal procedure law is a rather intricate issue [8]. Firstly, the legislator has no comprehensive and exhaustive position on this issue at the regulatory level. The Ukrainian legislator has not established a clear legal concept of e-evidence, particularly regarding its definition, type classification and features specific to e-evidence. Secondly, because of the ongoing and heterogeneous discussion among scholars regarding the prospects for institutionalising e-evidence in the legislative framework of criminal proceedings [9, 42; 10, 101].

At the doctrinal level, there are differences in the terminological approaches to the category of e-evidence. In particular, some scholars propose applying the concept of digital evidence, understanding it as factual data in the discrete (digital) form contained in certain physical storage and becoming available for perception after processing [11, 256]. Other scholars emphasise that the relevant definition is a purely theoretical category and understand electronic evidence as electronically stored information located on any physical storage, electronic devices or information systems [12, 182].

The issue of defining e-evidence in Ukrainian criminal procedure law resorts to the fundamental problem of placing this type of evidence among listed procedural sources of evidence in the Criminal Procedural Code of Ukraine (CPC), and its correlation with other types of evidence [13]. When studying a particular type of evidence, considering its essential characteristics and features, it is necessary to classify it according to a certain type of normative category. Ukrainian criminal procedure law knows the following types of evidence: testimony, expert findings, physical evidence, and documents [13, art. 84-2].

The CPC defines "Document" as a material object, which was created specifically for the preservation of information, such as an object containing information fixed by means of written signs, sound, image, etc., that can be used as evidence of the fact or circumstance which is established during criminal proceedings [13, art. 99-2]. On the other hand, a document is a material object created for a special purpose, which contains information recorded by signs, images, and sound and which can be used in criminal proceedings [13, art. 99-1]. Thus, the CPC defines e-evidence through the material prism, i.e., a specific list of objects (photo, video, audio, computer data) is defined through the generic category of document, which is a material object by its objective nature.

As a result, the Ukrainian legislator established certain sources of evidence in criminal procedure law and implicitly classified the concept of e-evidence under the document category. However, e-evidence has specific characteristics, i.e., it has, by nature, an uncertain appearance. By classifying electronic evidence under the category of "document", this category is connotated with digital objects, which are essentially coded and intangible information. Given its specific features, we can conclude that the CPC does not provide an optimal definition that considers the content of this particular type of evidence.

3. Contradictions and Crossroads: E-Evidence in Comparative Legal Contexts

The issue of e-evidence in Ukrainian criminal law should be considered in comparison with the approaches of other branches of procedure law to this issue. A holistic approach is justified because evidence is an integrated and multidisciplinary scientific field, even though the specifics of each form of legal proceedings must be considered. In this context, the Law of Ukraine No. 2147-VIII of 2017 amended the Civil Procedure Code of Ukraine (Civil Code), the Commercial Procedure Code of Ukraine (Commercial Code), the Code of Administrative Procedure (Administrative Code) [14]. It established a completely different approach to allocating and understanding the category of e-evidence than in criminal matters.

These codes define e-evidence as information recorded electronically that contains facts about the circumstances relevant to the case. A progressive step is the provision of a basic definition and the consolidation effect by emphasising "information in electronic form" as the fundamental principle in the definition of e-evidence. In this field of law, the Ukrainian legislator consequently sees e-evidence through the prism of the intangible information, which fully considers the nature and essential features of evidence in digitalised form. In addition, Law of Ukraine No. 2147-VIII of 2017 regulates the types of storage devices that may contain electronic information, including portable devices (memory cards, mobile phones), servers, backup systems, etc [14, para. 5]. The amendment of the Ukrainian law in said fields entails the novelty that written and electronic evidence is distinguished; in particular, if electronic evidence is submitted to the court in a paper copy, such information will not be considered paper evidence.

Thus, the relevant changes in the procedural legislation form a substantive placement of e-evidence in the system of sources of evidence in the Civil Code, Administrative Code, and Commercial Code. This is a conceptual advancement in understanding the specific phenomenon of e-evidence in Ukraine; simultaneously, it aligns the regulatory framework to the specific characteristics of e-evidence.

The described changes in Ukrainian legislation in civil, commercial and administrative law bring to light a substantive and systemic conflict with the position in Ukrainian criminal procedure law that, as explained, follows an understanding of e-evidence as a material document. At the same time, this approach directly negates the essence of electronic information as a key element of e-evidence. Therefore,

already these contradictions between the Ukrainian criminal procedure legislation and other branches of Ukrainian law reveal that (urgent) regulation is required that align the concept of e-evidence.

Given the specific and distinctive features of e-evidence, it cannot be attributed to any other category of evidence in Ukrainian criminal procedure legislation. Therefore there are grounds for legislative formalisation of the relevant novelties. Some scholars share this opinion regarding the legal consolidation of the e-evidence concept [15, 84].

4. Interaction of E-evidence with Other Evidence Types in Ukraine

4.1. E-evidence vs. traditional documents

One of the most important issues is the place of e-evidence in the system of evidence in Ukrainian criminal procedure, namely its correlation and distinction with the category of document. This approach has weaknesses.

Firstly, digital information is usually formed naturally and technically, *i.e.* without the intervention of a particular entity, but as a result of actions in the information network. A classic document is human-made.

Secondly, e-evidence and a document differ in their content. While a document contains written signs (text), diagrams, and drawings that are directly expressed tangibly, e-evidence may contain not only certain explicit digital information but also implicit information that is inaccessible to an ordinary user. For example, metadata, which is actually "data about other data," contains information about the modification of data, its creation, storage location, creator, *etc.*, and is principally unavailable without special permission.

Thirdly, a document as a set of information expressed in signs (text) directly connects with its physical storage. Given the peculiar nature and characteristics of digital information in terms of its ability to be freely copied and transmitted, e-evidence is not tied to specific physical storage, as it can be circulated via a network, reproduced simultaneously and on various devices, without losing its form and content.

4.2. Challenges of e-evidence on physical storage

Another problematic issue is the definition of e-evidence as a document in terms of its linkage to physical storage. Particularly, the CPC establishes the principle of connection between a document and physical data storage [13, art. 99-1].

According to the CPC, a document is not a specific digital object relevant to criminal proceedings, but its physical storage. In my opinion, the existing legislative provision causes practical difficulties, which particularly occur in the case of recording digital information. The provision of the CPC regarding the position of perception of a document through its physical storage violates the conceptual features of e-evidence. Firstly, e-evidence, by its technical nature, is autonomous in relation to physical storage; it can be created on certain physical storage but can also be displayed and stored on any device. Secondly, the CPC, is ambiguous in terms of evidential proof, i.e. the question arises of what needs to be examined during criminal proceedings: e-evidence or its physical storage?

In my opinion, both digital data relevant to criminal proceedings and the physical storage on which it is stored should be subject to examination. This answer to the question raised depends on the context of the e-evidence. If the physical storage includes digital or physical traces of a crime, then such a material object should be recognised as physical evidence. However, the physical storage in e-evidence should not matter if it is only a form of fixing digital information, provided that the key is to analyse the digital data, structure, components and metadata. Thus, the mandatory transfer of electronic evidence (digital information) to a separate physical storage is worth noting. In this regard, the fixation method will serve as a law enforcement tool for further examination of the evidence. For example, in cases where digital information cannot be reproduced in a tangible form, a special subject may record such information on a portable medium (optical disc, hard disk drive *etc*.). That is, one should proceed from the correlation between the concepts of 'form' and (or) 'content' of evidence in the context of their importance for criminal proceedings, which will determine whether digital information belongs to physical evidence or documents.

However, the current legislative framework, which enshrines the material principle of linking digital information, where the priority is given to physical storage, which may not be objectively relevant to criminal cases, is not applicable. In contrast, digital information is essential and goes beyond the scope of a document [13, art. 99]. It should be added, that the Criminal Court of Cassation of the Supreme Court of Ukraine, in case No. 751/6069/19, noted that physical storage is only a way of storing information, which is relevant only when an electronic document is physical evidence. The main feature of an electronic document is the absence of a rigid binding to a specific physical storage [16].

4.3. E-evidence vs. physical evidence

A special aspect is the issue of correlation and differentiation of e-evidence with the category of physical evidence. In the CPC, physical evidence is defined as follows: physical evidence shall mean tangible objects that have been used as a tool for committing a crime, retain traces of such or contain other information, which may be used as evidence of the fact or circumstance to be established during criminal proceedings, including the items that were an object of criminally unlawful actions, money, valuables or other articles obtained in a criminally unlawful manner or gained by the legal entity as a result of a crime [13, art. 98].

This definition of physical evidence also emphasises materiality. However, the object or subject of a crime can be objects of the material world and digital objects. Financial crimes can be committed with the emergence of new technologies, such as blockchain databases. Any conversion of illegally obtained crime proceeds can be implemented through various virtual assets (cryptocurrency, non-fungible tokens *etc.*). Furthermore, a situation can happen in which the object of a crime may be a computer virus, or the traces of criminal activity may contain metadata.

All of these digital (electronic) objects are intangible and may not be tied to specific physical storage that would include traces of a crime, and, therefore cannot be considered through the physical form of fixation. At the same time, the relevant objects themselves will be of direct relevance to criminal proceedings. Therefore, there is a need for a regulatory change in the concept of physical evidence by expanding it in terms of regulating the principle of non-materiality of objects that may be considered material evidence.

5. Navigating Possible Solutions: Addressing E-Evidence Challenges in Ukrainian Criminal Law

The analysis above demonstrated that collecting, storing, using and examining electronic evidence requires new approaches in Ukrainian criminal procedure. Action is required by the Ukrainian legislator who already attempted to tackle the issue of e-evidence in criminal procedure law: Draft Law No. 4004 of 2020, proposed that e-evidence should be defined as information in electronic or digital form that can be used as evidence of a fact or circumstance relevant to criminal proceedings [17]. In addition, this draft emphasises the classification of e-evidence, in particular, it includes electronic documents (text documents, graphic images, photographs, video and sound recordings); virtual assets; websites, web pages; text, multimedia and voice messages; metadata; databases. Unfortunately, this draft law did not take effect, and the issue of e-evidence remains unresolved until today.

Thus, we conclude that the current provisions of the CPC do not correspond to the fundamental features and nature of e-evidence. The fundamental issue is the impossibility of 'organic absorption' of e-evidence by category of document. After all, e-evidence is broader in nature and goes beyond the concept of a document. Also, in this context, it should be emphasised that the legislative regulation of the concept of e-evidence by giving preference to digital information rather than physical storage is the proper solution to the relevant issue.

We would like to note that the Ukrainian legislator should not only formulate a formal and theoretical definition and optimal classification of e-evidence but also a comprehensive regulatory framework that includes aspects of correlation with other types of evidence, principles of recording, evaluation and storage. This will contribute not only to the consistency of approaches to the regulation of evidence in procedural branches of law but will also serve to implement the fundamental principles, tasks and principles of criminal justice. Resolving the controversial issue of the category of e-evidence will eliminate several legislative conflicts and conceptual gaps, and prevent hypothetical manipulations and ambiguous interpretations of this type of evidence.

6. Conclusion

In conclusion, the legal analysis of the current state of play of Ukrainian legislation in criminal procedure demonstrated a pressing need for substantial improvements in the legal framework governing e-evidence. The existing landscape of e-evidence in Ukraine falls short of aligning with modern methodologies and standards, posing significant challenges to the criminal justice system's effectiveness. An ever-increasing reliance on digital technologies and electronic data characterises the contemporary world. In this digital age, criminal activities often leave electronic footprints that can be crucial in establishing guilt or innocence. However, the current state of e-evidence in Ukraine's criminal law is inadequate in adapting to the evolving nature of crime and technological advancements.

Enhancing the regulation and the express recognition of e-evidence is not merely a procedural formality; it is a cornerstone of effective law enforcement and the pursuit of justice. The absence of

robust legal provisions for electronic evidence can hinder the ability of law enforcement agencies and courts to investigate, prosecute, and adjudicate cases involving digital information, especially those related to war crimes in Ukraine. Moreover, the significance of improving the regulation of e-evidence extends beyond the immediate criminal justice context. In the post-war period, upholding the rule of law and ensuring accountability for past atrocities will be paramount. This requires a legal framework that can accommodate the complexities of e-evidence, ensuring that it is admissible, reliable, and subject to the necessary safeguards to protect individual rights.

Therefore, it is clear that establishing a more comprehensive and adaptable legal framework for e-evidence is a key imperative in Ukraine's pursuit of effective judicial prosecution in cases involving war crimes and the enduring supremacy of the rule of law in the post-war era. By aligning its legal system with modern approaches to e-evidence, Ukraine can better equip itself to address the challenges of the digital age and promote a fair and accountable judicial process.

REFERENCES:

1. Office of the United Nations High Commissioner for Human Rights. Ukraine: civilian casualty update 11 September 2023. URL: https://www.ohchr.org/en/news/2023/09/ukraine-civilian-casualty-update-11-september-2023.
2. Office of the Prosecutor General of Ukraine. International Crimes Committed During Russia's full-scale Invasion of Ukraine. URL: https://www.gp.gov.ua/.
3. Office of the Prosecutor General of Ukraine. If you became a victim or witness of Russia's war crimes, record and send the evidences! URL: https://warcrimes.gov.ua/en.
4. Office of the President of Ukraine. Russia-Ukrainian War. Evidences. URL: https://dokaz.gov.ua/.
5. Ukraine 5AM Coalition. Report a Crime. URL: https://www.5am.in.ua/en.
6. Anti-Corruption Headquarters. Russian War Criminals. URL: https://rwc.shtab.net/en.
7. eyeWitness to Atrocities. Welcome to eyeWitness. URL: https://www.eyewitness.global/.
8. Council of Europe. Webinar "Electronic evidence of war crimes". The role of journalists, media and social media. 25 November 2022. URL: https://www.coe.int/en/web/freedom-expression/electronic-evidence-of-war-crimes-webinar.
9. Riabushchenko, D. Conceptual and Theoretical Problems of the Category of "Digital (Electronic) Evidence" in the Criminal Process. *Economics.Finances.Law*, 2023. Issue. 5. P. 42–45. URL: https://doi.org/10.37634/efp.2023.5.9.
10. Shevchuk, V. The Role of Digital Technologies in the Investigation of War Crimes in Ukraine: Criminalistic Problems. *Grail of Science.* 2023. Issue 25. P. 97-101. URL: https://doi.org/10.36074/grail-of-science.17.03.2023.014.
11. Tsekhan, D. Digital Evidence: Concepts, Features and Place in the System of Proof. *Scientific Bulletin of the International Humanitarian University. Jurisprudence*. 2013. Issue 5. P. 256–260. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58.
12. Kalancha, I. and Stolitnii, A. Formation of the Institute of Electronic Evidence in the Criminal Process of Ukraine. *Problems of legality*. 2019. No. 146. P. 179. URL: https://doi.org/10.21564/2414-990x.146.171218.
13. The Criminal Procedural Code of Ukraine, № 4651-VI, 13 April 2012. URL: https://zakon.rada.gov.ua/laws/show/4651-17?lang=en.
14. Law of Ukraine No. 2147-VIII, 3 October 2017. URL: https://zakon.rada.gov.ua/laws/show/2147-19?lang=en#Text.
15. Kovalenko, A. Electronic Evidence in Criminal Proceedings: Current State and Prospects of Use. *Bulletin of the LDUVS named after E.O. Didorenko*. 2018. 4(84). P. 237–243.
16. Criminal Court of Cassation of the Supreme Court of Ukraine, 10 September 2020, Case 751/6069/19, para 15. URL: http://iplex.com.ua/doc.php?regnum=91722819&red=100003ad3e2380c6111ece3cbf7a26ca506213&d=5.
17. Draft Law "On amendments to the Criminal Procedure Code of Ukraine to improve the effectiveness of the fight against cybercrime and the use of electronic evidence", No. 4004, 1 September 2020. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771.