Electronic Evidence or Evidence in Electronic Form: Issues Behind the Rationale for Terminological Division

Kostiantyn Karaman *

* Doctor of Philosophy in Political Science, Doctoral student at NSC «Hon. Prof. M. S. Bokarius FSI», Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-2965-9661, e-mail: karamankostantin@gmail.com

DOI: 10.32353/khrife.1.2026.10 UDC 343.985(477)
Received: 13.02.2026 / Reviewed: 27.02.2026 / Accepted for print: 31.03.2026 / Available online: 31.03.2026

The Article aims to trace a correlation between the terms "electronic evidence" and "evidence in electronic form". The study examines their theoretical and legal disparities, practical utility of these terms within the framework of criminal proceedings, and seeks to formulate a scientifically grounded approach to their terminological division. The goal has been achieved through the comprehensive application of general scientific methods (analysis, synthesis and generalisation), as well as dialectical, logical-semantic, formal-legal, systemic-structural, comparative-legal, and hermeneutic methods. This paper analyses the current state of academic research into the legal nature of electronic information within the system of procedural sources of evidence, along with principal approaches to its terminological interpretation in criminal procedure doctrine. The focus is on distinctive features of digital data as data media capable of being reproduced repeatedly without changing content, leading to a debate on their relationship with traditional physical evidence and documents. It has been noted that the terms "electronic evidence", "digital evidence" and "evidence in electronic form" are used interchangeably in academic discourse, indicating a lack of a consistent approach to distinguishing between their meanings. Drawing on an analysis of legislative provisions and doctrinal propositions, the appropriateness of using the term "evidence in electronic form" has been substantiated, since it most accurately reflects the informational nature of digital data and aligns with the prevailing

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by Daryna Dukhnenko). The authors acknowledge translation as corresponding to the original.

framework of proving in criminal procedure. It has been concluded that the electronic form serves as a medium for evidentiary data, rather than constituting a standalone procedural category. Prospects for further research related to the development of uniform criteria for procedural identification of evidence operating in a digital environment have been outlined.

Keywords: *criminal procedure; pre-trial investigation; evidence; proof; electronic evidence; legal procedure.*

Research Problem Formulation

Today's fast-paced development of digital technologies and extensive use of electronic information systems in criminal proceedings have led to the emergence of new ways of recording and storing information of evidentiary value. Accordingly, in academic discourse and law application practice, the terms *electronic evidence*, *digital evidence* and *evidence in electronic form* are commonly used interchangeably, indicating a lack of a consistent approach to distinguishing between their meanings. The lack of clarity in terminology has made it difficult to develop a single doctrinal approach and has complicated the procedural qualification of relevant objects in criminal proceedings.

The issue of determining procedural nature of objects that are the target of criminal acts becomes challenging if these objects are electronic documents, software, or other forms of electronic information. Criminal law doctrine often recognises information itself (a constituent part of information infrastructure) as the subject of information technology offenses, thereby highlighting the need to revise conventional approaches to the physical nature of evidence and its procedural formalisation.

Intangible nature of electronic information complicates its correlation with traditional physical evidence, which is a tangible object. In criminal proceedings, parties involved in proving do not, in fact, deal with primary information, but rather with its representations: visualised data, graphic copies, or audio signals. It is therefore necessary for us to refine the conceptual framework, in particular the relationship between concepts that focus either on the technological nature of information (*electronic evidence*) or on the form in which it exists (*evidence in electronic form*).

Further academic discussion is also required to address the application of the traditional *physical evidence* concept—in particular its uniqueness—in a digital environment, where information can be reproduced multiple times without altering its content. These issues lead to a methodological inconsistency between classical criminal procedure constructs and current technological realities, directly impacting the choice of terminology and the determination of the legal nature of corresponding evidence.

Consequently, there is no agreed approach to the use of the terms *electronic evidence* and *evidence in electronic form*, as well as *digital evidence*. Accordingly, there is a need to comprehensively analyse their semantic relationship, identify theoretical and legal disparities, and develop a sound terminological approach that would be

consistent and relevant to the current context of criminal proceedings digitalisation.

Article Purpose

Determine the semantic relationship between the terminological constructs *electronic evidence* and *evidence in electronic form*, define their theoretical and legal disparities, and analyse practical utility of these terms in criminal proceedings, as well as formulate a scientifically grounded approach to their terminological division.

Research Methods

The specified goal was achieved through integrated application of methodological instruments, namely: philosophical, general scientific and specialised methods.

Dialectical method has contributed to exploring the development of scientific approaches to understanding the nature of electronic information in criminal proceedings, and to identifying contradictions between traditional procedural categories of proof and modern digital practices. Logical-semantic method has been employed to analyse the content of the terms *electronic evidence*, *digital evidence* and *evidence in electronic form*, facilitating the refinement of their semantic boundaries and the identification of distinctive features characterizing academic and regulatory usage of these terms.

Formal-legal (dogmatic) method has helped to study provisions of Ukraine's criminal procedure legislation, specifically the Criminal Procedure Code of Ukraine [1] (hereinafter referred to as the *CPC of Ukraine*), governing the system of evidence sources and the procedures for handling electronic information. Systemic-structural method has provided a deep dive into the role of electronic information within the broader framework of procedural sources of evidence, and has identified interrelationships between the categories of physical and electronic evidence.

Comparative and legal method have been applied to compare academic positions on the legal nature of evidence in electronic form and approaches to its classification. Hermeneutic method has been helpful in interpreting doctrinal concepts and legal rules, enabling us to identify their substantive focus and practical consequences for law application practice.

Generalisation has made it possible to systematise existing academic approaches and to formulate the author's view on the appropriateness of using the terminological construct *evidence in electronic form* as the one most consistent with both informational nature of digital data and the current model of criminal procedure proving.

Analysis of Essential Researches and Publications

The issue of evidence existing in the digital environment has taken centre stage in academic research over the last few years. Academic debate focuses on the procedural nature of electronic information, its place within the system of evidence sources, specific features of its collection, recording and assessment, as well as on the establishment of an appropriate terminological framework. Current legal doctrine remains divided on the legal nature of electronic (digital) evidence, resulting in a variety of approaches to its theoretical interpretation and practical application.

1 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 18.01.2026).

Researchers have made a significant contribution to the study of digital traces and evidence by focusing on interpretation of electronic (digital) information as a source of evidence, on identification of its forensic characterisation, and on challenges associated with its procedural formalisation. Scientific papers by O. Vakulenko [2], I. Kalancha [3], O. Kvashuk [4], A. Kovalenko [5], S. Kolomiitsev [6], O. Nikishev [7], V. Fihurskyi [8], M. Shcherbakovskyi and V. Sezonov [9], and other scholars have laid the theoretical framework for understanding digital traces as specific data media that are to be analysed and examined using special methods. These academic developments have demonstrated a shift in conventional forensic doctrine about traces, with a focus on integrating the digital component.

A separate research field is concerned with determining the place of electronic information within the system of procedural evidence sources. Certain researchers argue that it is appropriate to recognise electronic evidence as a distinct category of evidence, given its specific nature and the fact that it differs from documents and physical evidence. Notably, academic literature has put forward proposals to incorporate a distinct category of electronic evidence into the CPC of Ukraine and to develop specific procedural rules for handling such pieces of evidence. In contrast, another group of scientists views electronic information as a form of existing procedural sources—primarily documents—that does not necessitate the introduction of a new category of evidence.

2 Вакуленко О. Ф. Поняття властивостей доказів у кримінальному провадженні. *Право.ua.* 2021. № 4. С. 249—254. DOI: 10.71404/LAW.UA.2021.4.37 (date accessed: 18.01.2026).

3 Каланча І. Г. Докази електронної форми у кримінальному процесі України: теорія та практика : дис. … д-ра юрид. наук. Київ, 2025. 617 с. URI: https://elar.navs.edu.ua/handle/123456789/38317 (date accessed: 18.01.2026).

4 Квашук О. Д. Використання електронних доказів у кримінальному провадженні. *Центральноукраїнський вісник права та публічного управління.* 2025. Вип. 2 (10). С. 50—56. DOI: 10.32782/cuj-2025-2-5 (date accessed: 18.01.2026).

5 Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2022. Вип. 4 (100). С. 226—236. DOI: 10.33766/2524-0323.100.226-236 (date accessed: 18.01.2026).

6 Коломійцев С. О. Криміналістичні технології пошуку та фіксації комп'ютерних даних під час проведення слідчих дій : дис. … д-ра філос. в галузі права. Харків, 2025. 237 с. URI: https://dspace.univd.edu.ua/handle/123456789/24554 (date accessed: 18.01.2026).

7 Нікішев О. В. Цифрові (електронні) докази у кримінальному провадженні в умовах надзвичайних правових режимів. *Право.ua.* 2025. № 1. С. 365—371. DOI: 10.71404/law.ua.2025.1.54 (date accessed: 18.01.2026).

8 Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: Юридичні науки.* 2023. Вип. 4. С. 97—105. DOI: 10.32782/galician_studies/law-2023-4-14 (date accessed: 18.01.2026).

9 Щербаковський М. Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження. *Теорія та практика судової експертизи і криміналістики.* 2024. Вип. 2 (35). С. 10—27. DOI: 10.32353/khrife.2.2024.02 (date accessed: 18.01.2026) ; Щербаковський М., Сезонов В. Збирання та дослідження електронних документів із застосуванням спеціальних знань. *Там само.* Вип. 3 (36). С. 10—23. DOI: 10.32353/khrife.3.2024.02 (date accessed: 18.01.2026).

The issue of terminological clarity holds an important place in contemporary research. Research papers point out that concurrent use of the terms *electronic evidence*, *digital evidence* and *evidence in electronic form* is a sign of an evolving legal framework and the lack of a unified doctrinal position. In these circumstances, some authors emphasise the need for terminological division as a prerequisite for developing a uniform law application practice and for ensuring the cohesion within criminal procedural law.

Research focusing on digital traces as primary carriers of forensically relevant information plays a crucial role in the development of scientific thought. Contemporary criminalistics regards digital traces as a distinct category of information representations arising from users' interaction with the digital environment, capable of being transformed into admissible evidence provided they are properly recorded and verified. Such approaches support the idea that conventional understanding of evidence and its tangible nature should be re-evaluated.

There is an ongoing debate regarding the legal nature of digital data. Some researchers (A.-M. Anheleniuk [10], A. Kovalenko [11], A. Kryzhanovskyi [12], O. Metelev [13], D. Tsekhan [14]) insist that digital data should be treated as a separate category of evidence, while others (I. Kalancha [15], V. Fihurskyi [16]) argue that electronic nature of evidentiary information merely refers to the form in which it is recorded, and not to its standalone procedural category. This ongoing discourse confirms that contemporary academic thought is currently seeking a balanced approach that would reconcile the technical nature of digital data with the existing model of procedural proving.

Therefore, analysis of current academic research shows that considerable progress has been made in addressing theoretical and practical aspects of utilising electronic information in criminal proceedings. At the same time, the lack

10 Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 79. Ч. 2. С. 214—218. DOI: 10.24144/2307-3322.2023.79.2.32 (date accessed: 18.01.2026).

11 Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2018. Вип. 4 (84). С. 237—245. DOI: 10.33766/2524-0323.84.237-245 (date accessed: 18.01.2026).

12 Крижановський А. С. Критерії віднесення електронної інформації до видів доказів. *Аналітично-порівняльне правознавство.* 2025. Вип. 2. С. 1027—1032. DOI: 10.24144/2788-6018.2025.02.152 (date accessed: 18.01.2026).

13 Метелев О. П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* 2018. № 1 (20). С. 75—86. URI: http://biblio.umsf.dp.ua/jspui/handle/123456789/3159 (date accessed: 18.01.2026).

14 Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2013. № 5. С. 256—260. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc5/56.pdf (date accessed: 18.01.2026).

15 Каланча І. Г. Зазнач. твір. URI: https://elar.navs.edu.ua/handle/123456789/38317 (date accessed: 18.01.2026).

16 Фігурський В. М. Зазнач. твір. DOI: 10.32782/galician_studies/law-2023-4-14 (date accessed: 18.01.2026).

of consensus regarding the terminological definition of the phenomenon under study, various approaches to determining its procedural status, and insufficient consistency between forensic and procedural concepts call for further research into the relationship between the concepts *electronic evidence* and *evidence in electronic form.*

Main Content Presentation

The status of electronic information within the system of sources of evidence is set out in cl. 1 of Sec. 2 of Art. 99 of the CPC of Ukraine [17]. Analysis of these legal principles suggests that investigative (search) actions may yield information recorded in electronic form which shall possess independent evidentiary value. Consequently, researchers rightly observe that at this stage of criminal procedure, there are two main methods of incorporating electronic information into criminal procedural proving: seizure of a physical data medium or copying of relevant electronic (digital) data [18].

Analysis of characteristic features of electronic (digital) traces reveals that the main information contained therein can be entirely reproduced by copying or displaying the relevant computer data. The specified methods of procedurally introducing electronic information into the proving procedure are closely related to specific attributes of digital data, necessitating their separate analysis. For this reason, forensic approaches detailing types of digital information sources and conditions for their identification and recording within criminal proceedings become particularly valuable.

Classification of computer data and their storage media depends on a bunch of forensically relevant criteria, including characterisations of storage media, level of user's control over information, and significance of data for carrying out tasks in criminal proceedings, their role in the process of solving and investigating crimes, their accessibility and availability for examination and detection, as well as the evidence of malicious software activity. S. Kolomiitsev believes that main digital sources of computer data include log files, metadata, network traffic, data remanence, malware, information on user activity, and data stored in cloud environments. The researcher views these sources as potential data media capable of serving the process of proof in criminal proceedings [19]. The forensic approaches listed above are consistent with a fundamental technical feature of digital information: its ability to be reproduced repeatedly without altering its content.

Unlike physical traces, which are inherently unique and cannot be fully reproduced without losing their individual properties, computer data can be copied an unlimited number of times without altering its content, provided that technical requirements are met. Discrepancies between the original and the duplicate data usually concern only metadata, not affecting information content.

This feature is codified in provisions of Pts. 3 and 4 of Art. 99 of the CPC of

17 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 18.01.2026).

18 Крижановський А. С. Зазнач. твір. С. 1028. DOI: 10.24144/2788-6018.2025.02.152 (date accessed: 18.01.2026).

19 Коломійцев С. О. Зазнач. твір. URL: https://dspace.univd.edu.ua/handle/123456789/24554 (date accessed: 18.01.2026).

Ukraine [20], pursuant to which copies of electronic documents and computer data, drawn up in accordance with the procedure established by this Code, shall be recognised by the court as the original document. It shows that it is information itself, rather than the data medium on which it is recorded, that is recognised as having procedural significance. Given the fact that digital data can be reproduced and transferred between different technical environments multiple times, electronic traces are not rigidly tied to a specific physical medium. Their existence and nature are determined by the specific characteristics of computer systems, within which information is in constant circulation across various storage devices and information environments [21]. Accordingly, the medium primarily serves as a technical environment for information storage, whilst information content is decisive for proving a case. With this approach, it can be concluded that electronic (digital) traces should be regarded, first and foremost, as information phenomena that are not limited to a specific physical medium in terms of their procedural significance. At the same time, characteristics of the medium, method and time of data transfer, as well as technical conditions of storage play a supporting role in establishing to what extent information is reliable and authentic.

The indicated features of digital data logically lead to a discussion pertaining to their procedural nature and the feasibility of equating a physical data medium with physical evidence.

Although we agree that electronic information has a dual nature, we cannot accept that the recording of electronic data on a physical medium constitutes grounds for recognising it as physical evidence. We cannot, therefore, fully endorse A. Kryzhanovskyi's view that provisions of Sec. 1 of Art. 98 of the CPC of Ukraine [22] indicate that there is no direct legislative reference on the exclusion of electronic data media from the category of physical evidence [23]. We consider this reasoning to be insufficiently convincing, since "statutory silence" does not necessarily mean that the rules governing physical evidence automatically extend to electronic media or digital data. At the same time, it worth noting that this approach is not limited to unambiguous classification of electronic information solely as physical evidence, as the author also considers other possibilities for its procedural qualification.

A. Kryzhanovskyi proposes understanding electronic information as a document in cases where such data exhibit signs of a document. The criterion for distinguishing between physical evidence and a document is not the type of medium, but the nature and functional significance of information for criminal proceedings. For practical purposes, the author offers a system of classification criteria whereby electronic information may be classified either as physical evidence or as documents. From his perspective,

20 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 18.01.2026).

21 Коваленко А. В. Поняття та сутність … DOI: 10.33766/2524-0323.100.226-236 (date accessed: 18.01.2026).

22 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 18.01.2026).

23 Крижановський А. С. Зазнач. твір. DOI: 10.24144/2788-6018.2025.02.152 (date accessed: 18.01.2026).

these criteria are as follows: structure of electronic information (content and metadata), its documented nature, its functional role in proceedings, and information possessing qualities of physical evidence (use as an instrument of crime, evidence of criminal activity, status of the object of encroachment, etc.) [24].

Therefore, A. Kryzhanovskyi seeks to integrate electronic information into the existing system of procedural evidence sources without establishing a separate category of electronic evidence. His approach stems from the concept of physical and informational unity of evidence and is aimed at developing a practical algorithm for classifying electronic information within the existing model of criminal procedure.

It should be noted that evidence available in the digital environment plays a key role in criminal proceedings of this category, as per the position of the Supreme Court. Such materials include photographic evidence, audio and video recordings, other data media (including computer data), which may be stored in open information networks (internet resources, online media, social networks) as well as in restricted-access environments (private messaging apps, Telegram channels, personal email correspondence, data from mobile devices, flash drives, memory cards, etc.).

In its ruling of 21 July 2025 in Case No. 201/11849/23, the Supreme Court stated that provisions of Art. 99 of the CPC of Ukraine provide a basis for considering materials containing facts of unlawful acts committed by a person or groups of individuals, provided they have been obtained by authorised agencies with due observance of procedural requirements, as documents that may be used as evidence in criminal proceedings [25]. One of the procedural mechanisms for identifying and recording relevant information is inspection: *"Investigator or public prosecutor shall carry out visual inspection of the area, premises, items and documents and computer data"* (Pt. 1 of Art. 237 of the CPC of Ukraine) [26].

Law application practice has shown that it is possible to record digital information by examining websites and Telegram channels, with their content documented in an investigative (search) action record. During such an inspection, it is possible to take screenshots, download video files, photographs and other electronic materials, which are attached as appendices to the record drawn up in line with the requirements of the CPC of Ukraine. Provided that the inspection procedure is followed and proper procedural formalities are observed, courts recognise inspection records on websites and Telegram channels as valid and admissible evidence, since corresponding factual data has been collected in accordance with the procedure stipulated by the CPC of Ukraine [27].

Moving from theory to practice calls for a closer look at a procedural mechanism through which digital data can be-

24 Крижановський А. С. Зазнач. твір. DOI: 10.24144/2788-6018.2025.02.152 (date accessed: 18.01.2026).

25 Постанова Верховного Суду від 21.07.2025 р. Справа № 201/11849/23. Провадж. № 51-584км25 / ЄДРСР : вебсайт. URL: https://reyestr.court.gov.ua/Review/129086893 (date accessed: 18.01.2026).

26 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 18.01.2026).

27 Там само.

come valid and admissible evidence. We agree that the process of gathering and recording evidence in electronic form is linked to a specific investigative (search) action, where items and documents are seized or information is recorded by means of copying. This is precisely why researchers observe that only after verifying and evaluating obtained information in terms of its relevance, admissibility, and reliability does such information become evidence. Due to their legal nature, results of relevant procedural activities may be physical evidence or documents. That is why scientists believe that electronic data should be classified as physical evidence provided they are stored on physical media (they contain information capable of serving as evidence) [28]. Ongoing scientific debate necessitates a consideration of a broader range of doctrinal approaches regarding the place of electronic information within the system of procedural sources of evidence.

V. Fihurskyi's scientific paper notes that *"evidence in electronic form is information created, processed, stored or transmitted by means of analogue or digital signals, which is relevant to criminal proceedings"* [29]. The author points out that the specific nature of this information raises debate as to whether it should be included within the existing system of procedural sources of evidence in criminal procedure. The researcher identifies several key viewpoints on the legal nature of evidence in electronic form by analysing academic approaches. Under the first, such evidence is regarded as a type of document recognised under current criminal procedure legislation. Under this approach, electronic information (regardless of the form of a medium) can potentially be used as a document without having to be converted into another form. Criticising this approach, V. Fihurskyi aptly notes that it fails to fully address the specific nature of electronic information, which may serve not only as a data medium but also as a means of committing a criminal offence, an object of criminal encroachment, or evidence of criminal activity, thereby making it more similar to physical evidence. Under the second position, the author has concluded that evidence in electronic form is not a distinct procedural source, but rather a method of presenting evidentiary information. With this approach, digital materials may be regarded either as a form of physical evidence or as a combination of physical evidence and documentary evidence. The third approach, which V. Fihurskyi deems the most promising, involves recognising electronic evidence as an independent procedural source of evidence. Proponents of this approach argue that electronic information differs substantially from traditional documents in terms of how it is created, stored, and reproduced; it requires the use of specialised technical tools and can be edited, thus preventing it from being treated as equivalent to paper documents. Furthermore, they underscore the difference between electronic evidence and audio-visual materials, as the latter can only be a component of electronic information. Ultimately, V. Fihurskyi concludes that evidence in electronic form is a new socio-legal phenomenon of this information age, possessing distinct legal features and specific mechanisms of proof. Therefore, the

28 Крижановський А. С. Зазнач. твір. С. 1028—1029. DOI: 10.24144/2788-6018.2025.02.152 (date accessed: 18.01.2026).

29 Фігурський В. М. Зазнач. твір. DOI: 10.32782/galician_studies/law-2023-4-14 (date accessed: 18.01.2026).

author favours an approach whereby such evidence should be given a separate place within the system of procedural sources of evidence, alongside witness testimony, physical evidence, documents, and expert opinions [30].

An overview of these positions inevitably brings to the fore the issue of terminological clarity, as it is precisely the conceptual framework of a phenomenon that significantly influences the perception of its legal nature.

Given the ongoing terminological debate and taking into account the discussed features of digital information, it becomes evident that the phrase *evidence in electronic form* is more accurate. Thus, I. Kalancha uses the term *evidence in electronic form* instead of *electronic evidence* or *digital evidence*. In favour of the author's approach, we should note that she adheres to the principle of terminological accuracy and the necessity of avoiding conceptual confusion. A monograph focuses on the existence of various approaches—*electronic evidence*, *digital evidence*, and other derivatives—whilst emphasising that such a proliferation leads to terminological confusion, negatively impacting the needs of both academia and practice. It is for this reason that the author proposes terminological division as a prerequisite for establishing a unified legal position. I. Kalancha is also guided by provisions of the current CPC of Ukraine. She notes that, in criminal proceedings, electronic (or digital) evidence is not singled out as an independent procedural source of evidence. For this reason, the use of the *electronic evidence* term as a settled term could be premature or go beyond the scope of the current model of proof. In her dissertation, she also distinguishes between the *electronic* and *digital* aspects. The author refers to the academic view that *digital evidence* denotes the nature of information (binary code) from a technical perspective, whereas *electronic* refers to technical means of its creation and processing. Therefore, both terms contain an element of truth, but neither is universal. This is precisely why the scholar opts for the wording *evidence in electronic form* as a more neutral, procedurally sound term that:

- does not appear to be a separate category of evidence not provided for by the CPC of Ukraine;
- covers various digital representations of data;
- relates not to the new essence of evidence, but to the form of its existence and presentation;
- is consistent with the concept of the procedural nature of evidence in criminal proceedings.

Consequently, the concept *evidence in electronic from* is a compromise between the technical nature of the phenomenon and the procedural realities of criminal proceedings [31].

Analysis of academic approaches shows that the discussion is gradually shifting from the technical nature of digital data to the issue of their accurate terminological formulation within the framework of criminal procedure doctrine.

The approach advocating for the use of the *evidence in electronic form* term is therefore worth considering, as it emphasizes how evidence is stored rather than implying it is a separate type of evidence inherently connected to a specific medium.

30 Фігурський В. М. Зазнач. твір. DOI: 10.32782/galician_studies/law-2023-4-14 (date accessed: 18.01.2026).

31 Каланча І. Г. Зазнач. твір. URI: https://elar.navs.edu.ua/handle/123456789/38317 (date accessed: 18.01.2026).

Information-based nature of digital traces and their relative independence from physical media underpin the approach whereby electronic form characterises the manner in which evidence exists and is presented, rather than its independent procedural nature.

Conclusions

The research conducted confirms that advancement of digital technologies has fundamentally transformed traditional views on the nature of information possessing evidentiary value in criminal proceedings and led to the emergence of new approaches to its procedural formalisation. Analysis of current criminal procedure legislation and legal doctrine reveals that there is no uniform approach to defining the legal nature of electronic information and, consequently, to the application of the terms *electronic evidence*, *digital evidence*, and *evidence in electronic form*.

It has been proven that the specific characteristics of digital data—the ability to be copied repeatedly without altering their content, their relative independence from a physical medium, and the necessity of technical mediation for data accessibility—necessitate a rethinking of conventional approaches to classifying evidence based on its physical nature. In today's context, it is primarily data content that is of procedural significance, whereas a physical medium serves predominantly as a technical environment in which data exist.

Research into scientific perspectives has revealed the existence of several conceptual approaches to defining the place of electronic information within the system of sources of evidence: viewing it as a type of document, as a combination of physical evidence and documentary evidence, or as the separate, independent procedural source. However, analysis of the arguments regarding whether electronic information constitutes physical evidence has demonstrated that the lack of an explicit statutory prohibition cannot be regarded as sufficient grounds for extending the rules governing physical evidence to electronic information.

Under the current model of criminal procedural proving, electronic information is incorporated into the existing system of sources of evidence using the categories of documents and physical evidence, depending on how it was obtained and procedural formalities involved. This justifies the need for a rigorous terminological approach detailing not the creation of a new type of evidence, but the specific nature of evidentiary information.

Following the analysis, we have found that using the term *evidence in electronic form* is the most appropriate way to describe this concept, as it is best aligned with the informational nature of digital data and the current CPC of Ukraine. This wording avoids artificially singling out a distinct procedural framework, ensures terminological neutrality, and clarifies that electronic form refers to the manner in which evidence is stored and presented, rather than to its independent legal nature.

This means that terminological division between the concepts of *electronic evidence* and *evidence in electronic form* is of both theoretical and practical value, given that it has a direct impact on the procedural qualification of evidence and the choice of methods for its collection and evaluation in criminal proceedings. It is advisable to direct further research towards developing agreed criteria for procedural identification of evidence available in the digital environment, bearing in mind the rapid pace of information technology development.

Електронний доказ чи доказ в електронній формі: проблеми доречності термінологічного розмежування

Костянтин Караман

Мета статті — з'ясувати співвідношення термінологічних конструкцій «електронний доказ» і «доказ в електронній формі», визначити їх теоретико-правові відмінності та практичне вживання в кримінальному провадженні, а також сформулювати науково обґрунтований підхід до їх термінологічного розмежування. Поставлену мету реалізовано за допомогою комплексного застосування загальнонаукових (аналіз, синтез і узагальнення), діалектичного, логіко-семантичного, формально-юридичного, системно-структурного, порівняльно-правового та герменевтичного методів. Проаналізовано сучасний стан наукової розробленості проблеми правової природи електронної інформації в системі процесуальних джерел доказів, а також основні підходи до її термінологічного розуміння в доктрині кримінального процесу. Акцентовано увагу на особливостях цифрових даних як інформаційних об'єктів, здатних до багаторазового відтворення без зміни змісту, що зумовлює дискусійність їх співвідношення з традиційними речовими доказами й документами. Констатовано, що в науковому обігу паралельно вживають термінологічні конструкції «електронний доказ», «цифровий доказ» і «доказ в електронній формі», що свідчить про відсутність усталеного підходу до розмежування їхнього змісту. На підставі аналізу законодавчих положень і доктринальних позицій обґрунтовано доцільність застосування терміна «доказ в електронній формі» як такого, що найбільш повно відображає інформаційну природу цифрових даних і узгоджується з чинною моделлю кримінального процесуального доказування. Дійшли висновку, що електронна форма свідчить про наявність доказової інформації, а не про її самостійну процесуальну сутність. Окреслено перспективи подальших досліджень, пов'язані з виробленням єдиних критеріїв процесуальної ідентифікації доказів, що функціонують у цифровому середовищі.

Ключові слова: *кримінальний процес; досудове розслідування; докази; доказування; електронний доказ; процесуальна форма.*

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

Participants

The author has contributed solely to intellectual discussion underlying this document, case law research, writing and editing, and assumes responsibility for its content and interpretation.

Declaration of Competing Interest

The author declares no conflict of interest.

References

Anheleniuk, A.-M. Yu. (2023). Vykorystannia elektronnykh dokaziv u kryminalnomu protsesualnomu pravi Ukrainy (problemni pytannia) [The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues)]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*. Vyp. 79. Ch. 2. DOI: 10.24144/2307-3322.2023.79.2.32 [in Ukrainian].

Fihurskyi, V. M. (2023). Dokazy v elektronnii formi u kryminalnomu provadzhenni [Evidence in electronic form in criminal proceedings]. *Halytski studii: Yurydychni nauky.*

Vyp. 4. DOI: 10.32782/galician_studies/law-2023-4-14 [in Ukrainian].

Kalancha, I. H. (2025). *Dokazy elektronnoi formy u kryminalnomu protsesi Ukrainy: teoriia ta praktyka* [Evidence in electronic form in criminal proceedure of Ukraine: theory and practice] : dys. ... d-ra yuryd. nauk. Kyiv. URI: https://elar.navs.edu.ua/handle/123456789/38317 [in Ukrainian].

Kolomiitsev, S. O. (2025). *Kryminalistychni tekhnolohii poshuku ta fiksatsii komp'iuternykh danykh pid chas provedennia slidchykh dii* [Forensic technologies for searching and recording computer data during investigative actions] : dys. ... d-ra filos. v haluzi prava. Kharkiv. URI: https://dspace.univd.edu.ua/handle/123456789/24554 [in Ukrainian].

Kovalenko, A. V. (2018). Elektronni dokazy v kryminalnomu provadzhenni: suchasnyi stan ta perspektyvy vykorystannia [Digital Evidences in Criminal Proceedings: Current State and Prospects for Use]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka*. Vyp. 4 (84). DOI: 10.33766/2524-0323.84.237-245 [in Ukrainian].

Kovalenko, A. V. (2022). Poniattia ta sutnist elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia [The concept and essence of electronic (digital) traces of a criminal offenses]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka*. Vyp. 4 (100). DOI: 10.33766/2524-0323.100.226-236 [in Ukrainian].

Kryzhanovskyi, A. S. (2025). Kryterii vidnesennia elektronnoi informatsii do vydiv dokaziv [Criteria for attributing electronic information to types of evidence]. *Analitychno-porivnialne pravoznavstvo*. Vyp. 2. DOI: 10.24144/2788-6018.2025.02.152 [in Ukrainian].

Kvashuk, O. D. (2025). Vykorystannia elektronnykh dokaziv u kryminalnomu provadzhenni [The use of electronic evidence in criminal proceedings]. *Tsentralnoukraïnskyĭ visnyk prava ta publichnoho upravlinnia*. Vyp. 2 (10). DOI: 10.32782/cuj-2025-2-5 [in Ukrainian].

Metelev, O. P. (2018). Hnoseolohichna i pravova pryroda tsyfrovykh dokaziv u kryminalnomu provadzhenni [Gnoseological and legal nature of digital evidence in criminal process]. *Pravova pozytsiia*. № 1 (20). URI: http://biblio.umsf.dp.ua/jspui/handle/123456789/3159 [in Ukrainian].

Nikishev, O. V. (2025). Tsyfrovi (elektronni) dokazy u kryminalnomu provadzhenni v umovakh nadzvychainykh pravovykh rezhymiv [Digital (electronic) evidence in criminal proceedings under emergency legal regimes]. *Pravo.ua*. № 1. DOI: 10.71404/law.ua.2025.1.54 [in Ukrainian].

Shcherbakovskyi, M. (2024). Open Sources of Cyberspace as Objects of Forensic Research. *Theory and Practice of Forensic Science and Criminalistics*. Is. 2 (35). DOI: 10.32353/khrife.2.2024.02.

Shcherbakovskyi, M., Sezonov, V. (2024). Collection and research on electronic documents using specific expertise. *Theory and Practice of Forensic Science and Criminalistics*. Is. 3 (36). DOI: 10.32353/khrife.3.2024.02.

Tsekhan, D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concept, characteristics and place in the proof system]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Yurysprudentsiia*. № 5. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc5/56.pdf [in Ukrainian].

Vakulenko, O. F. (2021). Poniattia vlastyvostei dokaziv u kryminalnomu provadzhenni [The concept of key attributes of evidence in criminal proceedings]. *Pravo.ua*. № 4. DOI: 10.71404/LAW.UA.2021.4.37 [in Ukrainian].

Karaman, K. (2026). Electronic Evidence or Evidence in Electronic Form: Issues Behind the Rationale for Terminological Division. *Theory and Practice of Forensic Science and Criminalistics*. Issue 1 (42). Pp. 135—147. DOI: 10.32353/khrife.1.2026.10.