Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice

Gergana Varbanova
Nikola Vaptsarov Naval Academy, Varna, Bulgaria

Keywords

authenticity,
digital information,
digital technologies,
electronic evidence,
European legislation,
evidence,
judicial procedure,
law,
material evidence,
procedure

Abstract

Objective: to develop a new theoretical framework that challenges the traditional classification of electronic evidence as a subtype of material evidence and suggests considering it as a qualitatively new legal phenomenon with its own independent legal nature in the context of applicable European legislation.

Methods: the work uses the doctrinal method for the legal analysis of applicable European legislation, including Regulation (EU) 2023/1543 and Regulation (EU) 910/2014 (eIDAS), as well as their direct application in the national legal systems of the European Union member states. A comparative legal approach was used to identify differences between theoretical views and case law. A technological analysis of digital information was performed; specific examples were explained to illustrate the problems associated with the collection and use of electronic evidence within the European legislation framework.

Results: the author proposes a new doctrinal understanding of electronic evidence as an independent category that differs from traditional material evidence in its digital nature and specific characteristics. The introduction of European regulations requires rethinking the legal nature of electronic evidence as a qualitatively different legal phenomenon. It was established that treating electronic evidence as material one creates a risk of legal uncertainty, while the lack of appropriate legal regulation hinders effective law enforcement.

Scientific novelty: for the first time, the research proposes to overcome the established paradigm and identify electronic evidence as an independent

legal category in the system of evidence types. The article substantiates the unique digital nature of electronic evidence and the need to create an independent legal framework in various national legislations. It is proposed to improve scientific terminology using the term “electronic evidence”, which corresponds to the legal definitions in the legislation under study, instead of the outdated term “digital evidence”.

Practical significance: the work contains specific practical recommendations for the use of electronic evidence in the procedures for its identification, storage, presentation and analysis in various court proceedings in accordance with applicable supranational legislation. The research helps to overcome outdated ideas about the legal nature of electronic evidence and their incorrect identification with material evidence. This is important for effective law enforcement in the European Union member states.

For citation

Varbanova, G. (2025). Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice. *Journal of Digital Technologies and Law, 3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

Contents

Introduction

Electronic evidence has a special, different nature from other evidence that exists in the analog world and that certifies facts that occurred in the past, but are relevant to the present. The peculiarity of electronic evidence is due to the fact that it can remain unchanged over a long period of time, but can be dynamic, as its content can be different from the moment when the fact it certifies existed. It is difficult to trace, it can often be changed in order to conceal information or to deliberately alter it. Electronic evidence comprises digital information encoded as binary data (a sequence of ones and zeros), and it challenges legal theory and practice, intertwining legal knowledge with the technical features of this new legal phenomenon – electronic evidence. Digital information cannot

be considered as a material object, it cannot be perceived directly, it is not an object from the physical world, and this poses serious challenges to legal theory and practice.

This study proposes a new theoretical framework that challenges the traditional classification of electronic evidence as a subset of physical evidence. The author proposes a change in the paradigmatic understanding of the legal nature of electronic evidence and considers it as a new legal phenomenon that has its own independent legal nature and supranational regulation. The study focuses only on the applicable European legislation, including Regulation (EU) 2023/1543, Regulation (EU) 910/2014 (eIDAS), and the challenges that this new theory of the legal nature of electronic evidence poses.

The study uses the doctrinal method for legal analysis of the applicable European regulations and their direct application in the national legal systems of the Member States. A comparative approach is applied to clarify the differences between theoretical views and case law arising in the application of supranational legal norms. The analysis examines the technological aspects related to the nature of digital information and presents specific examples that illustrate the challenges in collecting and using electronic evidence in the context of European regulations.

This paper presents an effort to offer ways to overcome the old paradigm and to separate electronic evidence as an independent legal category in the system of types of evidence, as well as to distinguish it from physical evidence. The study presents arguments for the unique digital nature of electronic evidence and the need to create an independent legal framework in various national legislations. It is proposed to refine the scientific terminology by using the term «electronic evidence», which corresponds to the legal definitions given in the regulations under consideration, and to overcome the use of the outdated term «digital evidence».

1. The classical theory of physical evidence

The theory defines physical evidence as material objects that can reproduce facts relevant to the case or allow for the drawing of evidentiary conclusions about these facts. They refer to events that occurred in the past, but which have significance in the present and are related to the process of proving. For example, Mubarik (2019) considers as physical evidence any object, material, fingerprints or various substances (including bodily) collected from the crime scene that are relevant to the investigation and can contribute to clarifying the facts of the case. In order for an evidence to be qualified as physical, it is necessary that it has a material nature and can be perceived through one of the human senses . Some theorists argue that the physical medium carrying digital information. (e. g. disk, USB, hard drive) can be considered as physical evidence (Pastukhov, 2015; Dmitrieva & Pastukhov, 2023).

This traditional theory has shortcomings and is subject to serious criticism, because electronic evidence, considered as digital information, does not always have a material nature and can exist entirely in a digital environment, without being objectified on a physical medium – for example, records on a cloud server. Electronic evidence often does not exist in analog form and is not part of the material world in the classical sense of the term.

2. European regulatory framework applicable to electronic evidence

In an effort to define and unify the understanding of the specific legal nature of electronic evidence, the European Union adopted Regulation (EU) 2023/1543, which has direct application and provides a legal definition of the concept of "electronic evidence". Such a legislative decision is not accidental, but aims to overcome the different interpretations of the concepts in the national legislation of the Member States and to have a unified understanding on the legal nature of electronic evidence.

The Regulation defines "electronic evidence" as subscriber data, traffic data or content data stored by a service provider or on behalf of a service provider in electronic form. The legislative approach is neutral and does not provide an exhaustive list of all types of digital information that could be qualified as electronic evidence. The Regulation specifically focuses only on electronic evidence – digital information that is stored or transmitted by service providers in the context of their provision of digital services and for the purposes of criminal proceedings. Files or other digital data stored locally by users do not fall within the scope of Regulation (EU) 2023/1543. Such data may fall under the definition of "electronic documents" as per Regulation (EU) 910/2014 (eIDAS). when they contain information that is legally relevant for various civil, commercial, administrative or other public relations.

Regulation (EU) No 910/2014 (eIDAS) defines an "electronic document" as any content stored in electronic form, in particular in the form of text, sound, visual or audiovisual recording. In the context of eIDAS, an electronic document is a carrier of information in digital form which may be relevant to civil, administrative, commercial or other public relations. It is sufficient that the electronic document contains information which is legally relevant, regardless of whether the document was created accidentally or intentionally for the purposes of a particular legal relationship. Article 46 of Regulation (EU) No 910/2014 provides that an electronic document has the same evidentiary value as other evidence. The cited norm imperatively states that the evidentiary value of an electronic document cannot be denied solely because it is in electronic form, which, in turn, ensures certainty in cross-border disputes, including arbitration proceedings (Ferreira & Gromova, 2024). The Regulation practically obliges Member States

to recognize the validity of electronic documents as admissible evidence in various legal proceedings (Nekrošius, 2021; Daniel & Daniel, 2012)[1].

In the context of the study, the concepts of "electronic evidence" within the meaning of Regulation (EU) 2023/1543 and "electronic document" under Regulation (EU) 910/2014 should be compared. Electronic evidence under Regulation (EU) 2023/1543 covers a wide range of digital information – subscriber data, traffic data and content data, which may include structured or unstructured data, metadata or content of communications – and is distinct from electronic documents. The scope of Regulation (EU) 2023/1543 is limited to specific cases in criminal proceedings – for the preservation and provision of electronic evidence, and only in relation to digital information stored by or on behalf of service providers.

On the other hand, the concept of "electronic document" within the meaning of Regulation (EU) 910/2014 (eIDAS) has a narrower technological application, as it essentially refers to digital content perceived as a "document", but its legal applicability is significantly broader. The "electronic document" is not limited to the field of criminal proceedings, nor to data stored by specific service providers and is applicable across all branches of law: civil, commercial, administrative, and criminal. (Kirkov, 2022; Berube et al., 2025; Shin et al., 2025). Therefore, it can be concluded that electronic evidence under Regulation 2023/1543 represents a specialized type of digital information intended for the purposes of criminal proceedings, and has a narrower scope of regulation. In contrast, electronic documents under Regulation 910/2014 have a broader scope and significance, as their admissibility as evidence does not depend on the specific context of criminal proceedings, nor on the place of storage or the source of the data, but on compliance with the principles established by EU law for electronic identification, authentication and trust services, including the types of electronic signatures used in electronic documents.

It is noteworthy that the definition of "content data" under Regulation (EU) 2023/1543 and the definition of "electronic documents" under eIDAS are similar. The difference lies in the context and objectives, as "content data" under Regulation 2023/1543 is oriented towards digital information that is transmitted and stored by digital service providers and that should be preserved, respectively provided for the needs of criminal justice, while the definition of "electronic document" under eIDAS is related to the recognition of the legal value and use of electronic documents in all areas of public life.

The definition of electronic evidence within the meaning of Regulation (EU) 2023/1543 is not exhaustive, but only outlines some of the types of digital information that can be treated as electronic evidence. The approach is identical in the definition of the concept of "electronic document" under Regulation (EU) 910/2014 – any content stored in electronic

[1] Varbanova, G. (2020). Legal regime of electronic documents. Varna: Dangrafik Publishing.

form, in particular text, sound, visual or audiovisual recording. In both cases, the list is not exhaustive, taking into account that technologies are developing. When regulating public relations in the field of information technology, the legislative approach must be flexible, given the dynamics of technological development. Technological development implies the emergence of new types of electronic evidence and electronic documents, which cannot be excluded from the scope of Regulation (EU) 2023/1543 or eIDAS simply because they are not explicitly defined as electronic evidence or electronic documents, respectively.

3. Definition and legal nature of electronic evidence

Electronic evidence is a key tool in the evidentiary process, which requires a special approach to its collection, analysis and legal assessment. This approach must take into account the intensive development of technologies, as well as the specific features of electronic evidence in the context of the rule-making process (Begishev et al., 2020).

Until the adoption of Regulation (EU) 2023/1543, the theory defined electronic evidence as any information stored or transmitted in digital form that can be used as evidence. Traditionally, some authors assume that electronic evidence is physical evidence, since the information it contains is objectified on a specific material medium. According to this approach, it is the physical characteristics of the medium that determine the evidentiary value, and not the information itself (electronic evidence) recorded on it. Although initially plausible, this concept is flawed, because it does not take into account and does not reflect the specific nature of electronic evidence – as digital information, which has its own unique characteristics (Wu et al., 2025)[2].

In more recent research, there is also a theory that electronic documents are a special category of quasi-material evidence. According to (Bufetova, 2023; Guo, 2022), an electronic document as material evidence is a document that exists in electronic form, contains information relevant to the case, and is recorded on an electronic medium that allows the reproduction and use of this information in the process of proving. The very definition given by the author shows that an electronic document is considered a specific type – quasi-material evidence, in which the information contained in the material medium is important, and not its material characteristics.

This confusion arises from a misunderstanding of how digital information is generated, modified, stored and deleted. Digital information can be stored on various media – a hard drive, a USB device, a cloud, a server – or transmitted via electronic channels, but the information is not identical to the medium itself. A file can be stored on a computer or other technical medium, copied, transferred or deleted, but the computer

[2] Varbanova, G. (2024). The significance of electronic evidence in the context of cybersecurity and national security. Print Master Publishing.

or medium on which it is recorded does not constitute physical evidence, especially since the information may be recorded on a cloud server and accessed via a computer or other device.

From the definitions of electronic evidence and electronic documents it is evident that they do not have a material (tangible) nature, but represent a digital record, therefore they can be defined as a variety of intangible evidence (Vuchkov, 2023; Horsman, 2021). In order to be able to define electronic evidence as a new legal phenomenon, it is necessary to clarify their digital nature and the way in which digital information is created, transferred, stored, recorded and deleted.

Digital information is data in binary code – a series of zeros and ones processed by information systems (computer, smart device, etc.). Thus, text, images, sound or video recorded on a technical medium represent digital information in binary code that can be perceived by human senses through the use of generally accepted standards for converting and reproducing information, through which the zeros and ones are visualized as text, images or audio files.

To be admissible in court, the collection of electronic evidence must ensure the full integrity and identity of the information data, so as to guarantee its authenticity, the integrity of the content and the immutability of the data. Only when these requirements are met can electronic evidence be accepted as valid and reliable evidence in court proceedings.

4. Authenticity, integrity, and evidentiary value of electronic documents

The modern world is characterized by a continuous increase in legal relationships that arise, develop and terminate in an electronic environment. Every day, numerous contracts are concluded entirely electronically, consumers use online services, make electronic payments, and even legal proceedings are now carried out via videoconferencing and using tools of the electronic world. Almost all spheres of public and economic life are closely related to the use of electronic means of communication, processing and storage of information.

Cyberspace has become a commercial zone that transcends physical boundaries, but at the same time represents a center of attraction for committing numerous new and previously unknown computer crimes.

Electronic evidence – whether it is electronic documents, communication records, log files, metadata or other forms of digital information – is an integral part of legal relations in an electronic environment and is of essential importance for revealing crimes committed in cyberspace. Proving the facts, whether it is a question of civil or commercial legal relations, or of crimes committed in cyberspace, requires guaranteeing the authenticity, integrity and immutability of electronic evidence. This is achieved by implementing appropriate technical and organizational measures.

A key challenge in the presentation, analysis and admission of electronic evidence in legal proceedings – whether civil, criminal or administrative – is the authenticity, integrity and probative value of electronic evidence and electronic documents. In today's digital world, electronic evidence is becoming the most commonly used evidence. In order to be accepted as valid and reliable means of evidence, electronic evidence and electronic documents must satisfy several criteria, including the assurance of digital data integrity, in order to guarantee their authenticity, integrity and immutability.

An electronic document is considered authentic when its author, place and time of creation are established, and its content actually originates from the stated author and has not been altered since its creation (Surovtseva, 2020). In this sense, the authenticity and immutability of the electronic document can be ensured through the use of certification services under Regulation (EU) 910/2014 (eIDAS) – for example, a qualified electronic signature, a qualified electronic seal or a qualified electronic time stamp, which certify both the identity of the author and the time of creation and the integrity of the electronic document. The integrity of the electronic document or digital information can also be guaranteed through the use of blockchain technology and smart contracts, which provide the ability to store data in a decentralized, immutable and transparent environment (Miao et al., 2021). The blockchain ledger and its records ensure that the content of the electronic document has not been altered since its initial creation. The technology provides secure storage, protection against subsequent modification or deletion of the electronic document, as well as chronological verification of the records in the decentralized ledger, which guarantees the authenticity and traceability of electronic evidence (Al-E'mari et al., 2024; Stoykova, 2023).

Artificial intelligence (AI) systems can also be used in the evidence process, and in particular in the authentication phase of electronic documents, through automated content analysis, anomaly detection, version comparison and risk assessment, which enhances the security of handling electronic evidence. The integration of AI systems, blockchain technologies and qualified certification services creates a multi-layered mechanism for protecting the integrity and authenticity of electronic documents and electronic evidence, especially in the context of litigation and e-justice.

Conclusions

This study proposes a change in the traditional paradigm of understanding the legal nature of electronic evidence in the context of European legislation. Regulation (EU) 2023/1543 and Regulation (EU) 910/2014 (eIDAS) are analyzed, and the method of comparative legal analysis justifies the conclusion that electronic evidence cannot be equated with the traditional category of physical evidence, since it has a special, digital nature and unique technical characteristics. Electronic evidence is a new legal phenomenon that

must receive an independent legal regulation regarding the procedural actions related to its collection, storage, analysis and acceptance as a suitable means of evidence in the legal process. Considering electronic evidence as a type of physical evidence is not only incorrect, but also creates a real risk of legal uncertainty and difficulties in effective law enforcement in individual Member States. The study contributes to the development of the theoretical understanding of electronic evidence, consistent with applicable European law, while outlining opportunities for future research on the integration of emerging technologies such as blockchain and artificial intelligence in the process of proving and verifying the authenticity of electronic evidence.

The study proposes to overcome the old paradigm and to separate electronic evidence as an independent legal category in the system of types of evidence, as well as to distinguish it from physical evidence. The study presents arguments for the unique digital nature of electronic evidence and the need to create an independent legal framework in various national legislations. It is proposed to refine the scientific terminology by using the term «electronic evidence», which corresponds to the legal definitions given in the regulations under consideration, and to overcome the use of the outdated term «digital evidence».

The study provides specific guidelines of practical importance in the process of using electronic evidence – for the identification, storage, presentation and analysis of electronic evidence in various legal proceedings, in accordance with the applicable supranational law. At the same time, this study proposes to overcome outdated concepts regarding the legal nature of electronic evidence and its incorrect identification with physical evidence.

References

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. (In Russ.). https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Author information

Gergana Varbanova – PhD, Assistant Professor, Department of National Security and Information Technology Law, Nikola Vaptsarov Naval Academy
Address: 73 Vasil Drumev Street, Varna, Bulgaria
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 99, 2025
Date of approval – June 28, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика

Гергана Варбанова

Высшее военно-морское училище имени Николы Вапцарова, Варна, Болгария

Ключевые слова

аутентичность,
вещественные доказательства,
доказательства,
европейское законодательство,
право,
процессуальные действия,
судебное разбирательство,
цифровая информация,
цифровые технологии,
электронные доказательства

Аннотация

Цель: исследование направлено на разработку новой теоретической основы, которая бросает вызов традиционной классификации электронных доказательств как подвида вещественных доказательств и предлагает рассматривать их как качественно новый правовой феномен с собственной независимой правовой природой в контексте применимого европейского законодательства.

Методы: в работе применяется доктринальный метод для юридического анализа применимых европейских нормативных актов, включая Регламент (ЕС) 2023/1543 и Регламент (ЕС) 910/2014 (eIDAS), и их непосредственного применения в национальных правовых системах государств – членов Европейского союза. Для выявления различий между теоретическими взглядами и прецедентным правом используется сравнительно-правовой подход. Проводится технологический анализ цифровой информации и поясняются конкретные примеры, иллюстрирующие проблемы, связанные со сбором и использованием электронных доказательств в рамках европейского законодательства.

Результаты: автор предлагает новое доктринальное понимание электронных доказательств как самостоятельной категории доказательств, отличающейся от традиционных вещественных доказательств цифровой природой и специфическими характеристиками. Внедрение европейских регламентов требует переосмысления правовой природы электронных доказательств как качественно отличного правового явления. Установлено, что отношение к электронным доказательствам как к вещественным создает риск правовой неопределенности, а отсутствие соответствующего правового регулирования препятствует эффективному правоприменению.

Научная новизна: в исследовании впервые предлагается преодолеть устоявшуюся парадигму и выделить электронные доказательства как самостоятельную правовую категорию в системе видов доказательств. Обосновывается уникальная цифровая природа электронных

доказательств и необходимость создания независимой правовой базы в различных национальных законодательствах. Предложено совершенствование научной терминологии с использованием термина «электронные доказательства», соответствующего юридическим определениям в рассматриваемых нормативных правовых актах, вместо устаревшего термина «цифровые доказательства».

Практическая значимость: работа содержит конкретные рекомендации практического характера для использования электронных доказательств в процедурах их идентификации, хранения, представления и анализа в различных судебных разбирательствах в соответствии с применимым наднациональным законодательством. Исследование способствует преодолению устаревших представлений о правовой природе электронных доказательств и их неверного отождествления с вещественными доказательствами, что имеет важное значение для эффективного правоприменения в государствах – членах Европейского союза.

Для цитирования

Варбанова, Г. (2025). Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика. *Journal of Digital Technologies and Law*, *3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

Список литературы

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Информация об авторе

Варбанова Гергана– PhD, ассистент кафедры права в области национальной безопасности и информационных технологий, Высшее военно-морское училище имени Николы Вапцарова
Адрес: Болгария, г. Варна, ул. Василя Друмева, д. 73
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 19 июня 2025 г.
Дата одобрения после рецензирования – 28 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.