JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 4, Issue 2, April 2026 Online ISSN: 3030-3508
https://spaceknowladge.com

DIGITAL EVIDENCE IN JUDICIAL PROCEEDINGS: THEORY AND PRACTICE

Yusupova Shakhrizoda Shukhrat kizi
Bachelor, Sarbon University
Uzbekistan, Tashkent
e-mail: shakhrizoda0077@gmail.com

ARTICLE INFORMATION

ARTICLE HISTORY:

Received:13.04.2026
Revised: 14.04.2026
Accepted:15.04.2026

KEYWORDS:

international law, digital transformation, cybersecurity, digital rights, personal data, artificial intelligence, Uzbekistan, international cooperation.

ABSTRACT:

This paper explores the profound influence of digital transformation on the trajectory of international law. Central to this discussion is the contribution of international institutions, specifically the United Nations, in crafting norms and technical standards for the digital environment. The author evaluates pressing global concerns, including cybersecurity frameworks, personal data privacy, digital human rights, and the legal governance of artificial intelligence. Additionally, the research highlights systemic challenges such as escalating cyber threats and the imperative for harmonized global regulatory strategies. A significant portion of the study is dedicated to the legislative landscape of the Republic of Uzbekistan, detailing its digital reforms and the synchronization of domestic law with international requirements. The article concludes that the digital age necessitates strengthened global partnerships and the creation of resilient legal instruments to foster a secure and sustainable digital civilization.

Introduction

The current development of information technology is having a significant impact on the legal system. One of the most notable manifestations of this impact is the emergence and widespread use of digital evidence in judicial practice.

Whereas previously the focus was on physical and written evidence, today electronic data increasingly plays a key role: correspondence, CCTV recordings, mobile device data and other digital traces.

At the same time, law enforcement practice faces a number of challenges related to the assessment of such evidence. This is due to its specific nature: digital information is easily altered, copied and may be subject to manipulation. The study of digital evidence is becoming particularly relevant.

Main part

1. The Concept of Digital Evidence

There is no single, universally accepted definition of digital evidence in legal scholarship. However, most scholars agree that it refers to information existing in electronic form that is capable of corroborating facts relevant to a case.

Digital evidence includes:

- electronic documents;
- messaging app correspondence;
- audio and video recordings;
- server and database data;
- information from mobile devices.

In my view, an important feature of digital evidence is its intangible nature. Unlike traditional evidence, it does not have a physical form in the conventional sense, which complicates its perception and assessment by the court

2. Characteristics of digital evidence

2.1. Unlimited reproduction and verification of authenticity

The digital nature of information gives rise to its key property: the ability to be reproduced indefinitely. Unlike analogue media, where each subsequent copy inevitably leads to signal degradation and loss of clarity, digital data is duplicated with absolute precision at the binary code level. [1]

On the one hand, this characteristic significantly simplifies cross-border data exchange and speeds up law enforcement agencies' access to the evidence base. However, from the perspective of procedural law, the fact that a copy is identical to the original creates a serious

legal conflict. The absence of visible differences between the original file and its duplicate gives rise to high risks of forgery, unauthorised alteration of metadata, or the complete substitution of evidence. [2, 3]

In judicial practice, this requires the implementation of special verification mechanisms, such as:

- Hashing (Digital Fingerprinting): the use of algorithms (e.g. SHA-256) to record a unique 'fingerprint' of the data at the time of its seizure.
- Integrity checking: proof that not a single change was made to the data during the process of copying or storage.

Thus, the ease of copying renders digital information 'fragile' evidence, the legal validity of which depends directly on strict adherence to the chain of custody. [4]

2.2. Inherent vulnerability to modification and the latency of changes

One of the most critical characteristics of digital evidence is its high sensitivity to external interference. Unlike physical evidence, where tampering (such as erasure or alteration of a document) usually leaves physically detectable traces, digital information can be altered without leaving any traces visible to the naked eye.

Even the slightest alteration — replacing a single character in a text file, changing a pixel in an image, or adjusting a timestamp — can completely distort the evidential value of a document. The main difficulty lies in the latent nature of such alterations: the file's content remains visually unchanged, whilst its legal substance changes.

To neutralise this vulnerability within the context of legal proceedings, expert analysis methods must be employed:

- Metadata analysis: examination of metadata regarding the file's creation date, author, and revision history.
- Cryptographic verification: the use of digital signatures, which make it impossible to alter data imperceptibly once it has been recorded.

For a digital object to be accepted as evidence, it must first be confirmed that it has not been subject to destructive or deliberate modifications from the time of seizure until its presentation in court.

2.3. Technological dependence and hardware-software mediation

Digital evidence is, by its very nature, 'silent', as it cannot be perceived directly by humans through the senses. Unlike traditional written or physical evidence, information in a digital environment exists in the form of binary code, which requires technical interpretation.

This dependency is two-fold:

1. Hardware dependency: the need for specific equipment (servers, storage devices, specialised readers) to access the physical medium.
2. Software dependency: the use of specific software to decode and visualise the data.

The lack of suitable software or the use of obsolete file formats (legacy data) may result in the inability to reproduce the evidence in court. Furthermore, the very process of converting code into a human-readable form (for example, displaying log files as a table) creates a risk of subjective distortion of information by the software algorithm. This necessitates the involvement of technical specialists (forensic experts) in the process, who can guarantee that the data display methods used do not distort the original meaning of the data

2.4. Latency and the technological destruction of digital traces

A distinctive feature of the digital environment is the possibility of deliberately destroying or professionally concealing digital traces. Unlike traditional forensics, where the complete destruction of evidence (such as biological traces or murder weapons) is physically difficult, specialised tools exist in the digital realm for the irreversible deletion of data.The problem of concealing traces in legal proceedings manifests itself in several ways:

Use of anti-forensics: the use of software to 'wipe' free disk space, the use of steganography (hiding files within other files) or encryption that cannot be accessed without a key.

Remote destruction: the ability to remotely wipe mobile devices or cloud storage before they are physically seized by law enforcement agencies.

Manipulation of log files: professional tampering with system event logs, enabling an attacker to create a false alibi or divert suspicion onto third parties.

The difficulty of proving a case in such circumstances lies in the fact that the absence of a digital trail does not always mean that the act itself did not take place. This requires investigative authorities and the courts to resort to retrospective analysis — searching for indirect signs of system interference. Thus, combating 'digital camouflage' is becoming one of the priority tasks of international cooperation in the field of cybersecurity, particularly in the context of harmonising approaches to the preservation of evidence in the Republic of Uzbekistan and partner countries.

3. Classification of digital evidence

Digital evidence can be classified on various grounds:

By source:

- data from devices;
- information from the internet;

- data from cloud services.

By form of presentation:

- text-based;
- graphical;
- audiovisual.

By method of acquisition:

- voluntarily provided;
- obtained during investigative proceedings;
- extracted using specialised technology.

This classification allows for a more precise understanding of the specific characteristics of working with each type of evidence.

4. Procedural and technical aspects of digital evidence consolidation

The collection of digital evidence constitutes the most critical phase of criminal or civil proceedings, characterised by a heightened risk of data loss. Any deviation from established regulations at this stage may result in the evidence being deemed inadmissible due to a breach of the principle of legality. To ensure the legal validity of digital evidence in court, strict compliance with a set of requirements is necessary:

1. Strict procedural legitimacy: Data collection must be carried out exclusively within the framework of the law, whilst respecting citizens' constitutional rights (for example, the right to privacy of correspondence). In the context of digital transformation, this requires a clear distinction between 'inspection of the scene' in physical space and 'access to data' in cloud storage.

2. Logging and verification of actions: Every stage of interaction with a digital medium — from physical seizure to software-based copying — must be recorded in detail in a log. It is recommended to video-record the seizure process to rule out suspicions of the deliberate planting of false files.

3. Ensuring immutability (data integrity): A fundamental requirement is the creation of a 'bit-stream image' of the storage medium. The expert's work must be carried out solely on the copy, whilst the original is placed in a sealed storage facility. The use of hashing algorithms (checksums) enables the court to verify that the information presented is identical to that which was originally seized.

Working with digital information requires a synergy of legal knowledge and technical expertise. In the practice of the Republic of Uzbekistan, this raises the issue of training judges and investigators in digital forensics, which is the key to a fair trial in the digital age.

5. Criteria and conflicts regarding the admissibility of digital evidence

In modern jurisprudence, the issue of the admissibility of digital data is central. Judicial scrutiny of the legitimacy of such evidence is based on three 'pillars', the verification of which is critical to the outcome of the case:

1. Lawful origin: The evidence must have been obtained in strict accordance with the provisions of the Code of Criminal Procedure or the Code of Civil Procedure. Any violation of the right to privacy or the confidentiality of correspondence during the collection of data renders it legally invalid.
2. Content integrity: The court must satisfy itself that the content of the file has not been subject to any overt or covert alteration since its creation or discovery.
3. System integrity: It is important to prove that no technical distortion of the data occurred during its transmission and storage.

In practice, proving the absence of interference (negative proof) becomes a complex task requiring the use of cryptographic checksums and a detailed description of the 'chain of custody'.

6. Methodology for assessing the reliability of digital evidence and the role of expert expertise

Assessing the reliability of digital evidence requires comprehensive verification. The court cannot limit itself to a mere visual assessment of the information; it is obliged to take into account:

- Identification of the source: verification of the originator and the device from which the data was sent.
- Circumstances of capture: the conditions under which and the technical means by which the information was captured.
- Technological verification: the presence of log files, metadata and other system-based confirmations of the event's authenticity.

In this context, the forensic technician becomes a key figure in the process. Their specialist knowledge enables the court to overcome the 'technological barrier' and interpret digital code as a reliable legal fact.

7. The Specifics and Dynamics of Law Enforcement Practice in Uzbekistan

The legal system of the Republic of Uzbekistan is actively adapting to the challenges of the digital age. The country's judicial practice is increasingly relying on non-traditional forms of evidence, including:

- Messages from messaging apps (Telegram, WhatsApp) as evidence of contractual obligations or threats.
- Data from intelligent video surveillance and biometric identification systems.
- Geolocation and transaction data from mobile banking apps.

Nevertheless, this process is undergoing active transformation. The main limiting factor remains the lack of standardised best practices for the seizure and presentation of such data, which sometimes leads to ambiguous court rulings.

8. Systemic barriers and risks in the use of digital evidence

The analysis identifies key factors that hinder the effective use of digital information in the justice system:

- Lack of standardisation: The absence of clear legislative criteria for assessing 'digital authenticity'.
- Skills gap: Insufficient digital literacy among some members of the judiciary and investigative services.
- Threat of deepfakes: The rise of AI technologies enabling the creation of voice and video forgeries indistinguishable from reality.
- Jurisdictional barriers: Extreme difficulty in obtaining evidence stored on foreign servers (Cloud Evidence) or in encrypted form.

9. Prospects for development

In the coming years, the role of digital evidence will only grow. This is linked to the ongoing digitalisation of society.

Promising areas:

- the implementation of blockchain technologies;
- the development of digital forensics;
- the creation of uniform standards for data handling;
- the professional development of specialists.

In my view, it is precisely the standardisation of procedures that will significantly improve the effectiveness of digital evidence.

Conclusion

To summarise the findings of this study, it must be noted that digital evidence has definitively evolved from a supplementary tool into a fundamental element of modern justice. Against the backdrop of the rapid digitalisation of social relations, its role will continue to grow steadily, driven by the shift of a significant portion of human activity into the virtual realm. [1, 2, 3] Nevertheless, the effective integration of digital information into the

evidentiary system requires the implementation of a comprehensive strategy covering three key areas:

Legal adaptation: There is a need to move away from attempts to adapt traditional norms towards the creation of an autonomous legal framework that takes into account the unique properties of digital objects — their intangibility, fragility and ease of replication. Legislation must clearly regulate procedures for the seizure of data from cloud storage and the use of blockchain technologies to ensure its immutability.

Technological standardisation: The success of law enforcement depends directly on the implementation of uniform forensic standards for data collection and storage. The mandatory use of hashing algorithms and adherence to a strict 'chain of custody' must become indisputable conditions for the admissibility of evidence.

Organisational and human resources development: Technological progress requires the training of a new generation of lawyers with interdisciplinary knowledge. The establishment of specialised units of 'digital experts' and the improvement of the judiciary's digital literacy are key to preventing expert errors and ensuring the right to a fair trial.

For the Republic of Uzbekistan, the current stage is decisive. The successful implementation of international standards in digital forensics and the harmonisation of national legislation will not only enhance the effectiveness of the fight against cybercrime but also create a reliable legal environment for the sustainable development of a digital society. The future of justice is inextricably linked to its ability to embrace technology whilst remaining the guarantor of the rule of law and human rights in the digital age.

Bibliography

1. Convention on Cybercrime (Budapest, 23 November 2001) // Collection of International Treaties. — [International standard on digital evidence].
2. Criminal Procedure Code of the Republic of Uzbekistan // National Database of Legislation of the Republic of Uzbekistan (Lex.uz).
3. Law of the Republic of Uzbekistan 'On Cyber Security' dated 15 April 2022 No. ZRU-764.
4. Decree of the President of the Republic of Uzbekistan 'On Measures for the Further Introduction of Digital Technologies into the Justice System' dated 3 September 2020 No. PP-4818.

5. Bernovsky I.V. Problems with the use of digital evidence in criminal proceedings // Russian Legal Journal. — 2021. — No. 3.
6. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. — 3rd Edition. — Academic Press, 2011. — 840 p.
7. Carrier B. File System Forensic Analysis. — Addison-Wesley Professional, 2005. — 600 pp.
8. Mason S., Seng D. Electronic Evidence. — 4th Edition. — Institute of Advanced Legal Studies, 2017. — 380 pp.
9. https://www.unodc.org
10. https://truescreen.io
11. https://digitalevidence.ai
12. https://cellebrite.com
13. https://rjsaonline.com
14. https://www.ojp.gov
15. https://www.researchgate.net
16. https://www.researchgate.net
17. https://ejournal.seaninstitute.or.id
18. https://www.researchgate.net
19. https://www.researchgate.net
20. https://inlibrary.uz
21. https://www.amu.apus.edu
22. https://www.researchgate.net
23. https://pmc.ncbi.nlm.nih.gov
24. https://www.researchgate.net
25. https://www.researchgate.net
26. https://pmc.ncbi.nlm.nih.gov
27. https://www.communitylawfirm.com
28. https://www.researchgate.net
29. https://africanjournalofbiomedicalresearch.com
30. https://www.researchgate.net