American Journal of Alternative Education
ISSN: 2997-3953 (Online)
Vol. 2, No. 10, Oct 2025,
Available online at: https://scientificbulletin.com/index.php/AJAE

Legal Assessment and Utilization of Digital Evidence in Pre-Trial Proceedings: Foreign Experience

Badalboev Feruz Yusufovich
Deputy Head of the Organizational Department, Head of the Legal Support Directorate,
Ministry of Internal Affairs of the Republic of Uzbekistan

Article information:
Manuscript received: 15 Aug 2025; **Accepted:** 20 Sep 2025; **Published:** 31 Oct 2025

Digital evidence is significant not only for its collection and preservation but also for its legal evaluation. The proper assessment of digital evidence during pre-trial proceedings serves as the foundation for investigative bodies and courts to make lawful decisions.

The theory of digital evidence is well-developed in the criminal procedural legislation of foreign countries. It is understood as information stored or transmitted in binary (digital) form[1]. Recently, authors have been highlighting the tendency of digital evidence to expand in volume, become more complex, easily modifiable, and more accessible to all individuals. Consequently, the methods of working with such evidence are also being refined[2]. In foreign scientific circles, there is already discussion about “computer” or “digital forensics”.

International organizations play a crucial role in developing regulations for digital evidence. Notably, in 2019, Interpol conducted its first online training dedicated to digital evidence. The training identified key challenges in obtaining evidence in digital format, including from foreign sources, and developed recommendations for legislative and law enforcement agencies of member states.

Among the experiences of foreign countries, Western European nations are of particular interest. In particular, on April 17, 2018, the European Commission put forward two important legislative initiatives to improve the mechanisms for the cross-border collection and use of electronic evidence.

These legislative initiatives aim to regulate processes related to electronic (digital) evidence within the European Union territory on a unified legal basis, as well as to ensure effective cooperation among law enforcement agencies.

Various approaches to this issue exist in European Union countries. Notably, in 2017, the Federal Republic of Germany enacted the “Law on Ensuring Rights in Social Networks,” which mandates providers to designate an authorized person responsible for receiving information requests from law enforcement agencies within the country[3]. The law stipulates fines of up to 500,000 euros for failing to appoint a representative or not responding to law enforcement inquiries. Additionally, the legislation requires social network providers to report illegal content to the Federal Criminal Police Office.In 2021, the Law “On Combating Legal Extremism and Hate Crimes” was adopted, which further developed the provisions of the 2017 law[4].

[1] Interactive Tool for Ranking Digital Evidence Needs / by Brian A. Jackson, Dulani Woods. URL: https://www.rand.org/pubs/tools/TL175.html
[2] Information Technology in the Criminal Procedure of Foreign Countries / D.V. Bakhteev, A.I. Zazulina, V.A. Zadorozhnaya [et al.]. – 1st ed. – Moscow: Yurlitinform, 2020.
[3] Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). URL: http://www.bmjv.de/DE/Themen/ FokusThemen/NetzDG/NetzDG_node.html
[4] Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminal URL:https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=%2F%2F%2A%5B%40attr_id=%27bgbl121s0441.pdf%27%5D

Such measures are currently being discussed only in Italy. Belgium, on the other hand, does not require a company representative to be present in its territory, but strives to ensure compliance with regulations by foreign providers through internal procedures.

In general, the draft documents of the European Union shorten the timeframes for utilizing evidence and ensure direct cooperation with service providers. Providers and individuals whose data is being requested will have access to specific legal protections. The EU documents also reinforce guarantees of fundamental human rights, including the right to protection of personal data. Overall, it is emphasized that law enforcement agencies will no longer be dependent on the voluntary willingness of IT companies. The documents also facilitate access to digital evidence stored outside the European Union.

In 2019, the Council of the European Union granted the European Commission two mandates to negotiate international agreements: a) with the United States to facilitate access to digital evidence, including the development of conflict-of-law rules and general rules for the direct transfer of evidence; b) with the Council of Europe to join the Additional Protocol to the 2003 Budapest Convention on Cybercrime. The negotiations are currently ongoing with varying degrees of success[5].

In December 2020, Europol, Eurojust, and the European Judicial Network published a report on the status of digital evidence in the European Union. The report emphasizes that cross-border access to information is crucial for conducting an increasing number of investigations into a wide range of crimes (including economic offenses, drug trafficking, human trafficking, cybercrime, and sex-related crimes). The report provides examples of successful investigations and highlights the problems that exist at the national level in various EU countries.

In the United States, the issue of utilizing digital evidence has received considerable attention. The foundations of this practice began to emerge in the late 1970s. Early judicial decisions established that, for computer data to be admissible as evidence, there must be sufficient and reliable grounds to ensure their authenticity[6].

For example, in *United States v. Scholle*, the court held that the prosecution had provided the necessary grounds by demonstrating that the computer data concerning narcotics had been systematically collected. Furthermore, the prosecution presented the sources of the computer program and the input control procedures, which guaranteed the accuracy and reliability of the information obtained. On this basis, the defendant was convicted, with digital evidence serving as one of the grounds for the judgment.

In the 1980s, the use of digital evidence was officially permitted in judicial practice. Such evidence included e-mails, digital photographs, ATM transaction logs, text documents, instant messaging histories, accounting software files, internet browser histories, databases, information stored in computer memory, backup copies, printed documents, Global Positioning System (GPS) tracking data, electronic hotel door lock logs, as well as digital video and audio files[7].

Several rules governing the use of digital evidence were developed. In particular, participants in proceedings were required to demonstrate: the reliability of computer hardware; the method of inputting initial data; the measures taken to ensure the accuracy of the data entered; the procedures for storing data and preventing their loss; the reliability of the computer programs used for data processing; and the safeguards established to verify the accuracy of such programs.

---

[5] URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/189

[6] Biryukov, P. N. On Evidence in the Criminal Procedure of the USA // Legal Standards of State Power and Law Enforcement Activities: Construction, Organization, Implementation, Effectiveness: Proceedings of the International Scientific and Practical Conference Dedicated to the 100th Anniversary of the Faculty of Law of Voronezh State University (Voronezh, November 15–16, 2018): in 2 parts / ed. by Yu. N. Starilov, O. S. Rogacheva. Voronezh: Voronezh State University Publishing House, 2019. Part 2. Pp. 69–76.

[7] Hart A. In court, digital evidence can shine or fizzle // The Atlanta JournalConstitution. 2014, July 26 ; Goodison S. E., Davis R. C., Jackson B. A. Digital evidence and the U.S. criminal justice system. Research Report № RR-890-NIJ. Santa Monica, CA: RAND, 2015.

At the same time, courts in different U.S. states interpreted the authentication of digital evidence, the "best evidence rule," and related principles differently. Digital evidence was also frequently criticized, primarily due to its susceptibility to alteration. However, in recent years, courts have increasingly rejected such objections. For example, the U.S. court in *United States v. Bonallo* held that "the mere possibility of altering data on a computer is not sufficient to render such evidence unreliable"[8].

At present, under the revised Federal Rules of Evidence of the United States, the provisions of the Rules apply to digital evidence in the same manner as to traditional documents. The key issue concerning digital evidence remains its admissibility. In the U.S., digital (electronic) data are often deemed inadmissible by courts if obtained without judicial authorization. In most states, a warrant is still required to seize and examine digital devices. This requirement may cause complications in investigations when evidence of other crimes is discovered.

For example, the widely cited *Schroeder* case illustrates this problem: investigators, while examining the defendant's computer in relation to another crime, discovered child pornography images. However, in order to bring charges on this ground, they were required to obtain a second warrant.

As is well known, digital evidence is rarely presented in a format convenient for reading. This requires law enforcement agencies and courts to take additional steps to use such materials as evidence. It is often necessary to "produce a hard copy" of the material. In U.S. criminal procedure this issue is governed by the *best evidence rule*.

If a party seeks to introduce a document for which the original is not available, that party must provide a satisfactory explanation to the court demonstrating the absence of the original. If the original cannot be produced and the court finds the explanation acceptable, the party may be permitted to use secondary evidence to prove the contents of the document and to admit that evidence as competent proof.

In particular, courts have held that printouts of computer-stored information do not necessarily violate the best evidence rule. Where a printout accurately and fully reflects the content of the electronic information, it may be treated procedurally as the "original" for evidentiary purposes.

As a result, Rule 1001(d) of the *Federal Rules of Evidence* was revised to state:

"For data stored in electronic form, an 'original' means any printout—or other output readable by sight—if it accurately reflects the data. An 'original' of a photograph includes the negative or a print from it."

Furthermore, Rule 1001(e) defines a *duplicate* as:

"A counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."

According to Rule 1003, "A duplicate is admissible to the same extent as the original unless a genuine question is raised about the authenticity of the original, or in the circumstances it would be unfair to admit the duplicate in lieu of the original."

Rule 1004 of the Federal Rules of Evidence supplements the provisions on the "Best Evidence Rule" by establishing exceptions. According to this rule, the original document is not required, and its contents may be proved by other forms of evidence in the following circumstances:

(a) when all originals have been lost or destroyed, provided that this did not result from the bad-faith actions of the party; **(b)** when the originals cannot be obtained by any available judicial process; **(c)** when the original is in the possession of the opposing party, who, after being duly notified that its production in court is required, fails to produce it; **(d)** when the writing, recording, or photograph is not directly related to a central issue in dispute.

[8] Federal Rules of Evidence 2020. URL: https://www.law.cornell.edu/rules/fre (составляют одну из федеральных частей «УПК США»).

Although the Criminal Procedure Code of the Russian Federation does not expressly recognize digital evidence as an independent type of evidence, it provides that digital data collected during various procedural actions and subjected to forensic examination may subsequently be admitted in court as legally valid evidence.

In practice, digital evidence in Russia is primarily derived from the following sources: electronic documents, telephone records, e-mail correspondence, video surveillance recordings, messenger communications.

According to the norms of the Criminal Procedure Code, such information is initially collected by investigative bodies and its authenticity and reliability must be confirmed through forensic examination. For instance, data obtained from e-mail correspondence may not be recognized as admissible evidence in court if it has not undergone expert examination. Therefore, in Russian practice, the procedural validity of digital evidence requires the use of technical examinations, computer-forensic analyses, and specialized software and technical tools.

At the same time, in Russian judicial practice, the assessment of the authenticity and legality of digital evidence largely depends on its source, the process of collection, and the conditions of preservation. If procedural rules are violated during the collection of digital evidence, or if its integrity is compromised, the court may refuse to accept such evidence.

Scholars emphasize that the collection of digital evidence differs from that of traditional physical evidence and requires an entirely different set of knowledge and skills. Attention is drawn to the fact that there are numerous methods for extracting digital evidence from various computer devices. Both the methods themselves and the devices on which such evidence is stored are rapidly evolving.

The preservation of digital evidence also constitutes a complex task: unlike material evidence, it can be altered or destroyed. Investigators must be able to confirm the authenticity of digital evidence and provide documentation verifying its integrity. They are also required to improve their own computer literacy and to involve specialists and experts in the process.

Considering the rapid development of information technologies and the growing prevalence of cybercrime, the use of foreign experience in handling digital evidence is of great importance for the activities of investigative bodies of the Republic of Uzbekistan. Uzbekistan has already taken significant steps in this direction; as evidence, one may refer to Law No. ORQ-1003 adopted in November 2024, which formally recognized digital data as admissible evidence.

The significance of foreign experience can be described in the following areas: First, the improvement of legislation and regulatory frameworks is manifested in the detailed regulation of procedures for working with digital evidence. Foreign practice may assist in developing more advanced norms governing the collection, registration, seizure, preservation, examination, and presentation of digital evidence. This includes specific requirements to ensure the integrity and reliability of digital data, such as the use of metadata, hashing, and the documentation (protocolization) of all stages of handling digital information.

Second, the regulation of the use of innovative technologies. This relates to rapidly evolving technologies such as blockchain, artificial intelligence, and the Internet of Things, which may serve as potential sources of digital evidence. Studying how other countries adapt their legislation to these challenges will enable Uzbekistan to establish a legal foundation in advance.

Third, the utilization of experience in cross-border cooperation. Since crimes in the digital sphere often have a transnational character, the effective investigation of such cases requires international cooperation in the exchange, transfer, and provision of digital evidence and mutual legal assistance. In this regard, foreign experience plays a decisive role.

Another promising direction in the use of foreign experience is the development of technical and expert capacities. This is associated with the introduction of advanced forensic tools and software. The study of

software products and hardware solutions applied in developed countries for the collection, analysis, and visualization of digital evidence (for example, systems similar to those of the Belarusian company "Sled" JSC, which have already been examined by representatives of Uzbekistan) provides an opportunity to implement similar or even more advanced systems[9].

Another important area is the training and professional development of specialists in the field of information and digital technologies. This requires engaging foreign experts to conduct training and seminars, as well as organizing internships for investigators, forensic experts, and prosecutors of the Republic of Uzbekistan in countries where digital forensics is well developed. Such measures will allow them to acquire advanced methods of detecting, collecting, preserving, and analyzing digital traces.

Thus, the issues of discovering, examining, evaluating, and using digital evidence remain at the center of attention of investigative and judicial bodies in foreign states. It is evident that the criminal process and the science of digital forensics in Uzbekistan must thoroughly study the experience of international organizations and foreign states. This experience may be effectively utilized both in the process of sending requests for legal assistance and in obtaining digital evidence from foreign countries for the purposes of criminal investigations.

REFERENCES:

1. Interactive Tool for Ranking Digital Evidence Needs / by Brian A. Jackson, Dulani Woods. URL: https://www.rand.org/pubs/tools/TL175.html
2. Information Technology in the Criminal Procedure of Foreign Countries / D.V. Bakhteev, A.I. Zazulina, V.A. Zadorozhnaya [et al.]. – 1st ed. – Moscow: Yurlitinform, 2020..
3. Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). URL: http://www.bmjv.de/DE/Themen/ FokusThemen/NetzDG/NetzDG_node.html
4. Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminal URL:https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=%2F%2F%2A%5B%40attr_id=%27bgbl121s0441.pdf%27%5D
5. Biryukov, P. N. On Evidence in the Criminal Procedure of the USA // Legal Standards of State Power and Law Enforcement Activities: Construction, Organization, Implementation, Effectiveness: Proceedings of the International Scientific and Practical Conference Dedicated to the 100th Anniversary of the Faculty of Law of Voronezh State University (Voronezh, November 15–16, 2018): in 2 parts / ed. by Yu. N. Starilov, O. S. Rogacheva. Voronezh: Voronezh State University Publishing House, 2019. Part 2. Pp. 69–76.
6. Hart A. In court, digital evidence can shine or fizzle // The Atlanta Journal Constitution. 2014, July 26 ; Goodison S. E., Davis R. C., Jackson B. A. Digital evidence and the U.S. criminal justice system. Research Report № RR-890-NIJ. Santa Monica, CA: RAND, 2015.
7. Federal Rules of Evidence 2020. URL: https://www.law.cornell.edu/rules/fre (составляют одну из федеральных частей «УПК США»).
8. Zinovyeva, E. S. International Cooperation on Ensuring Information Security: Problems, Actors, Prospects: Dissertation for the Degree of Doctor of Historical Sciences: 23.00.04 / E. S. Zinovyeva. – Moscow, 2017. – 332 p.

[9] Zinovyeva, E. S. International Cooperation on Ensuring Information Security: Problems, Actors, Prospects: Dissertation for the Degree of Doctor of Historical Sciences: 23.00.04 / E. S. Zinovyeva. – Moscow, 2017. – 332 p.