Vital Annex: International Journal of Novel Research in Advanced Sciences
ISSN: 2751-756X
Volume 05 Number 02 (2026)
https://innosci.org/IJNRAS

Article

The Emergence and Historical Development of the Need to use Electronic Evidence

Abdullayev Akmaljon Yo'lchiboyevich[1], Saidov Jurabek Jalolovich[2]

1. Lecturer of the Department of Preliminary Investigation and Inquiry, Law Enforcement Academy of the Republic of Uzbekistan
2. Master's Student, Law Enforcement Academy of the Republic of Uzbekistan

Abstract: This article provides a comprehensive analysis of the emergence and development of the use of electronic evidence. It examines the formation of cybercrime in the context of information technology development, the first instances of the use of electronic evidence, their procedural significance, and the stages of their recognition in international and national legislation. Special attention is given to the development of electronic data and digital evidence in the legislation of the Republic of Uzbekistan, as well as issues related to ensuring their admissibility.

Keywords: Evidence, Electronic Evidence, Digital Evidence, Electronic Data, Pre-Trial Proceedings, Information Technology

1. Introduction

At a videoconference meeting held on January 19, 2021, under the chairmanship of the President of the Republic of Uzbekistan, Shavkat Mirziyoyev, devoted to improving the system of spiritual and educational work and strengthening cooperation between state and public organizations, special emphasis was placed on educating youth in the spirit of patriotism and national pride, as well as on the importance of studying history and expanding scientific research in this area[1].

It is well known that understanding the essence of any social phenomenon or reality primarily requires a thorough study of its historical roots and developmental origins. In this regard, examining the stages of emergence and development of the concept of electronic evidence contributes to the effective use of such evidence in law enforcement practice, ensures the integration of theory and practice, and facilitates further improvement of this institution[2].

In today's context of globalization and the rapid advancement of information and communication technologies, development must keep pace with these dynamic changes. Electronic evidence represents a new type of evidence that has emerged in the era of information and communication technologies.

It is evident that for any concept or institution to be reflected in legislation, there must first be a practical need for it. The historical necessity for the use of electronic evidence in the process of collecting, verifying, and evaluating evidence during pre-trial proceedings is directly linked to the introduction and widespread integration of information technologies into society[3].

Citation: Yo'lchiboyevich A. A. and Jalolovich S. J. The Emergence and Historical Development of the Need to use Electronic Evidence. Vital Annex: International Journal of Novel Research in Advanced Sciences 2026, 5(2), 76-84.

Received: 17th Jan 2026
Revised: 26th Jan 2026
Accepted: 21th Feb 2026
Published: 30th Mar 2026

2. Materials and Methods

This study is based on a comprehensive qualitative research approach aimed at analyzing the emergence and development of electronic evidence. The research methodology includes historical, comparative-legal, and system-structural methods.

The historical method was applied to examine the stages of formation and evolution of electronic evidence, starting from the early manifestations of cybercrime to the development of modern digital forensics and legal frameworks. This allowed identifying key milestones and transitional phases in the use of electronic data in criminal proceedings[4].

The comparative-legal method was used to analyze international and national legal acts, including legislative practices of foreign countries and the Republic of Uzbekistan. Through this method, similarities and differences in the regulation of electronic evidence were identified, as well as the process of its recognition as an independent type of evidence.

The system-structural method enabled the study of electronic evidence as an integral element of criminal procedural activity. It was used to determine the interrelation between technological development, cybercrime, and legal regulation.

In addition, the study relies on the analysis of scientific literature, legal documents, and practical cases related to the use of electronic and digital evidence. This combination of methods ensures a comprehensive understanding of the research problem and supports the validity of the conclusions drawn[5].

3. Results and Discussion

Indeed, while people initially perceived information technologies as tools that simplify life, increase efficiency, save time, and facilitate everyday activities, over time it became apparent that their negative consequences could outweigh their benefits. More importantly, these consequences are often more severe and widespread than other forms of harm. Today, approximately one in seven individuals worldwide reports that their personal data, capable of damaging their honor and dignity, has been leaked onto the Internet, that their communications and family secrets have been accessed by entities such as intelligence services, or that their financial resources have been unlawfully withdrawn by unknown persons.

In modern conditions, digital devices such as smartphones, computers, servers, and cloud services have become primary sources of traces of criminal activity. Without these technologies, it is virtually impossible to conduct an effective investigation[6].

In light of the above, it is necessary to examine the factors that led to the emergence of the need to use electronic evidence, to determine in which country crimes involving information technologies were first committed, when and where crimes were first solved using electronic evidence, and which country first incorporated the concept of electronic evidence into its legislation. In other words, it is essential to analyze the historical development and evolution of electronic evidence.

As a result of the rapid development of information technologies, a new form of crime—cybercrime—has emerged. According to scientific literature, the first unlawful acts committed using electronic means date back to the 1960s in the United States, particularly at the Massachusetts Institute of Technology (MIT), where students engaged in unauthorized interference with telephone networks through so-called "phone phreaking".

Although these actions were not initially fully recognized as crimes from a legal perspective, they are considered the earliest manifestations of cybercrime.

Subsequently, in 1971, the "Creeper" program appeared on the ARPANET network, becoming the first program capable of self-replication across a network. This marked a new stage in the development of offenses committed through computer networks[7].

Cybercrime began to take on a more serious and practical dimension in the 1980s. In particular, in 1986–1987, cases of unauthorized access by German hackers to U.S. military and scientific networks were recorded. Within the framework of these cases, computer logs, network activity traces, and digital data were used for the first time as evidence in the course of criminal investigations.

In 1988, the "Morris Worm," created by Robert Morris, spread widely across the Internet, causing a significant portion of the network infrastructure to fail. During the investigation of this case, network logs (log files), software code analysis, and other electronic data were presented as primary evidence in court. This case is considered one of the first instances demonstrating the practical criminal procedural significance of electronic evidence.

Examining the history of the concept of electronic evidence, it can be noted that it emerged as a result of the formation and development of computer-related crimes. In the late 1980s and early 1990s, U.S. law enforcement agencies, in the process of detecting and investigating electronic crimes, introduced the concept of electronic (digital) evidence into scientific discourse [8].

The practice of using electronic evidence also originated in the United States, particularly in the detection of crimes in the banking and telecommunications sectors, where electronic transactions, server logs, and other digital data began to be widely used . This led to the necessity of recognizing electronic data as a form of evidence.

Starting from 1984, the FBI Laboratory and other U.S. law enforcement agencies began actively engaging in the investigation of computer-related crimes.

In this regard, the Computer Fraud and Abuse Act (CFAA) was adopted in the United States in 1986, which criminalized unauthorized access to computer information and recognized electronic data as an object of legal protection.

In 1998, directors of U.S. federal forensic laboratories conducted extensive research on a new field of forensics related to computer technologies. On May 12, 1998, a research group led by Dr. Don Kerr (Deputy Director of the FBI Laboratory), Mark Pollitt (Head of the FBI Computer Analysis Team), and Scott Charney (Head of the Computer Crime and Intellectual Property Section at the Department of Justice) conducted studies on digital audio, digital video, and computer forensics. Following extensive scientific discussions, they agreed to unify computer-related crime and computer forensics under the term "digital forensics" (digital evidence) [9].

The difficulties associated with investigating computer-related crimes prompted U.S. law enforcement agencies to intensify efforts in combating such offenses. As a result, specialized training centers such as the Federal Law Enforcement Training Center (FLETC) and the National White Collar Crime Center (NW3C) were established. These centers developed various training programs aimed at equipping law enforcement personnel with the skills necessary to investigate crimes committed using computer technologies, emphasizing the importance and application of electronic (digital) evidence in such investigations.

Subsequently, a new branch of legal science—digital forensics—emerged and developed rapidly.

One of the major achievements in the field of digital forensics is the publication of the book "Digital and Multimedia Sciences" by the American Academy of Forensic Sciences on February 20, 2008. This work presents scientific information on the key advancements and achievements in digital forensics over the preceding 28 years.

Speaking of forensic science in general, it is understood as a field that encompasses tactical and methodological approaches, as well as scientific and technical tools, used in accordance with the requirements of criminal procedural law for the detection, collection, preservation, and examination of evidence in order to solve and prevent crimes[10].

Accordingly, digital forensics is a field of science that encompasses activities related to the detection and investigation of crimes committed using computer technologies and information systems.

In general terms, digital forensics can be defined as a scientific discipline aimed at the identification, collection, processing, analysis, and interpretation of data stored in electronic (digital) form.

Electronic (digital) evidence constitutes an integral component of nearly all types of crimes, and both electronic evidence and digital forensics play a crucial role in enabling law enforcement agencies to establish the truth in criminal proceedings.

Subsequently, in order to regulate this field at the international level, the Council of Europe adopted the Convention on Cybercrime (Budapest Convention) in 2001, which established general principles for the collection, preservation, and presentation of electronic (digital) evidence.

It is well known that the emergence of the need to use electronic evidence is directly related to the existence of technical devices that leave traces capable of being evaluated as electronic evidence. Therefore, it is appropriate, first of all, to determine when such technical means began to be used.

M.S. Sergeev traces the historical roots of the use of technical means in evidentiary activities back to the 16th century, specifically to the invention of the camera obscura. According to the author, particular significance should be attributed to the 1882 circular order of the Police Department of the Russian Empire, which established the official procedure for the use of photography and photographic recording methods. In his view, this historical document can be regarded as the formal starting point for the use of technical (including proto-electronic) devices in criminal proceedings[11].

However, in our view, it is not appropriate to consider the 16th century as the starting point or a stage in the development of the use of electronic data and their storage media in evidentiary processes, as suggested by the author. This is because the camera obscura is an optical device that allows an inverted image of external objects to be projected through a small aperture, and it was primarily used in the fields of art and astronomy.

It should be acknowledged that photography indeed began its practical development in the mid-19th century and was widely used as an important tool for documenting certain procedural activities in criminal proceedings. However, it would be incorrect to regard this process as a stage in the development of the use of electronic data and their carriers in pre-trial proceedings. This is because electronic data refers to digital information generated, stored, and processed by electronic devices based on binary code (0 and 1). Photography, on the other hand, is a traditional (mechanical) process based on chemical reactions and is not directly related to electronic technologies[12].

In this regard, we believe that the actual starting point for the use of electronic data and their storage media in pre-trial proceedings should be associated with the introduction of audio recording technologies in the conduct of procedural actions within criminal procedural legislation.

Thus, by the Decree of the Presidium of the Supreme Soviet of the RSFSR dated August 31, 1966, "On Amendments and Additions to the Criminal Procedure Code of the RSFSR," Article 141 was introduced into the Code, entitled "Use of Audio Recording during Interrogation," which legally established the procedural rules for the use of audio recording in the course of interrogations. This development created, for the first time in criminal procedural practice, a formal legal basis for recording and preserving information using electronic means[13].

Furthermore, beginning from the second half of the 20th century, video recording and cinematographic techniques started to be widely used to ensure effective documentation of the results of investigative actions. Crime scene inspections, interrogations, identification procedures, and a number of other investigative activities began to be recorded using video equipment. In particular, these technologies made it

possible to store evidentiary information for extended periods using electronic storage media such as magnetic tapes and videocassettes.

Notably, during this period, audio recordings were фикced through electromagnetic impulses (magnetic oscillations), which provides grounds to consider this stage as the actual beginning of the use of electronic data and their storage media in pre-trial proceedings. This process involved the storage of electronic signals on physical media (magnetic tapes), their subsequent reproduction, and their use for procedural purposes[14].

Starting from the 1990s, with the rapid development of electronic computing machines, their capabilities began to be widely utilized across various sectors of society, including pre-trial proceedings. During this period, electronic data storage media such as hard drives, floppy disks, and compact discs were впервые introduced into criminal procedural practice, enabling the storage, processing, and transmission of investigative information in digital form.

The rational use of electronic computing technologies contributed to a more comprehensive, objective, and efficient conduct of proceedings, facilitated the recording of evidence, simplified procedural activities, and improved the overall quality of proof. In addition, new forms of using electronic data emerged at the stage of preliminary investigation, including the preparation of procedural documents using computers, the creation of electronic archives, and the development of digital photography and video recording.

Following the independence of the Republic of Uzbekistan, its Criminal Procedure Code was adopted on September 22, 1994. The legal framework for the use of audio recording, video recording, and cinematographic techniques in the conduct of procedural actions was established in a number of provisions of the Code, including Articles 19 (Public hearing of criminal cases), 69 (Specialist), 81 (Types of evidence), 91 (Auxiliary methods of recording evidence. Annexes to the protocol), 106 (Recording the course and results of interrogation), 136 (General rules for inspection), 151 (Protocol of exhumation), 155 (Procedure for conducting an experiment), and 426 (Minutes of the court session) [15].

The legal basis for the widespread and systematic use of electronic data and their storage media in pre-trial proceedings was further strengthened by the Law of the Republic of Uzbekistan dated April 18, 2018, "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan." This law introduced the concept, procedure, and grounds for the use of videoconferencing in a number of provisions of the Criminal Procedure Code, including Articles 19, 114 (Procedure for interrogation of witnesses and victims), 318 (Procedural costs), 418 (Postponement of court proceedings), and 426.

Subsequently, the Law of the Republic of Uzbekistan dated May 23, 2019, "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Related to Ensuring the Protection of the Rights of Participants in Criminal Proceedings," introduced significant changes in the use of electronic data and their carriers at the pre-trial stage. In particular, the Code was supplemented with Articles 91–91, which established the procedure for the use of videoconferencing in pre-investigation checks, inquiry, and preliminary investigation. These legislative changes created a legal basis for the remote collection of electronic data, their storage in digital form, and their procedural formalization[16].

Furthermore, the Law of the Republic of Uzbekistan dated January 12, 2021, "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan," introduced procedures for the use of audio recording in the course of criminal proceedings.

Thus, the legal framework governing the use of electronic data and their storage media at the pre-trial stage has been consistently developed and expanded within national legislation. As a result, modern information technologies have become an integral

component of criminal procedural activity, and a comprehensive legal framework for handling electronic evidence has been established.

In particular, the Law of the Republic of Uzbekistan dated May 14, 2020, "On Amendments and Additions to the Criminal Procedure Code of the Republic of Uzbekistan Aimed at Strengthening the Protection of the Rights and Freedoms of Citizens Participating in Criminal Proceedings," introduced additional provisions regulating the procedure for conducting investigative actions that must be mandatorily recorded by means of video recording[17].

These amendments provided a new content to Article 91 of the Criminal Procedure Code, stipulating that in cases involving especially serious crimes, the following investigative and procedural actions must be formally documented using video recording: crime scene inspection, search, verification of testimony at the scene, investigative experiment, detention of a person, waiver of defense counsel, personal search conducted during detention, and seizure.

Finally, in the 21st century—an era characterized by rapid scientific and technological advancement—the concept of electronic (digital) evidence has emerged in legal science. Due to the inherent characteristics of such data, including their hidden nature, high level of confidentiality, and complexity, as well as the difficulty of their comprehensive identification and use, modern criminals increasingly commit various offenses in cyberspace using computer technologies.

In turn, this factor has also directly affected the Republic of Uzbekistan, placing a significant responsibility on law enforcement agencies to ensure the comprehensive, objective, and effective investigation of crimes committed using computer technologies[18].

For the first time in the legislation of the Republic of Uzbekistan, the concept of "electronic evidence" was mentioned in the Presidential Decree No. PF-6256 dated July 5, 2021, adopted with the aim of further improving the forensic examination system and introducing new types of expertise and research. The list approved by Annex 4 of this Decree assigns tasks for the introduction, during 2021–2025, of expert examinations and research specifically related to electronic evidence.

Subsequently, paragraph 8 of the "Roadmap," approved by the annex to the Resolution of the President of the Republic of Uzbekistan dated November 30, 2023 (No. PQ-381), on improving the system for combating offenses committed using digital technologies and protecting the rights of consumers of digital products (services), provides for the task of defining the concept of "electronic (digital) evidence," as well as establishing procedures for their identification, collection, examination, expert analysis, evaluation, recording, and storage, along with determining the rights and obligations of participants involved in these processes[19].

Based on the implementation of the tasks предусмотренные in this Resolution, it was stipulated that amendments and additions be introduced into legislative acts concerning the definition of the concept of "electronic (digital) evidence," as well as the procedures for identifying, collecting, presenting, examining, evaluating, recording, and storing electronic evidence, along with determining the rights and obligations of participants in these processes.

As a result of the reforms carried out, taking into account the rapid development of information technologies in society and arising from objective necessity, the Law of the Republic of Uzbekistan dated November 21, 2024, "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System of Working with Digital Evidence" (No. ZRU-1003) , introduced the concepts of electronic data and digital evidence into the criminal procedural legislation of the Republic of Uzbekistan, thereby establishing clear legal norms governing electronic data and digital evidence[20].

This Law introduced into criminal procedural activity such concepts as "electronic data" (Article 204) and "digital evidence" (Article 204), and provided a detailed regulation of the procedures for their collection, submission, inspection, examination, and evaluation.

According to the Law, electronic data are data created, processed, and stored using electronic devices, information systems, and information technologies. Digital evidence, in turn, refers to electronic data containing information relevant to the case, including electronic files, audio and video recordings, data stored on the Internet, as well as other forms of electronic data.

Furthermore, with the adoption of this Law, the role of electronic data and their storage media in the stages of pre-investigation checks, inquiry, and preliminary investigation was strengthened. In particular, it was established that the participation of a specialist is mandatory during the seizure, search, and inspection of electronic objects, and the principles of preserving the integrity and authenticity of digital evidence were granted legal force.

At present, the use of electronic data and their storage media at the stage of pre-trial proceedings has reached such a level that, in some cases, procedural actions carried out and recorded without the use of modern technologies may lose their admissibility. In particular, investigative actions in cases of especially serious crimes that are not documented by video recording, electronic data obtained without the participation of a specialist, or data collected from electronic storage media where the integrity of digital evidence has been compromised may be признаны inadmissible evidence[21].

Proceeding from this, in accordance with Resolution No. 14 of the Plenum of the Supreme Court of the Republic of Uzbekistan dated June 23, 2025, "On Amendments and Additions to Resolution No. 24 of August 24, 2018, 'On Certain Issues of the Application of Criminal Procedural Legislation on the Admissibility of Evidence,'" paragraph 9 of Resolution No. 24 of August 24, 2018, states that evidence shall be considered inadmissible if it is obtained in violation of the requirements of the Criminal Procedure Code, including cases where data contained on digital (electronic) storage media are seized or examined without the participation of a specialist.

Thus, the emergence and development of the necessity of using electronic data and their storage media at the stage of pre-trial proceedings in the Republic of Uzbekistan have undergone several key stages as a historical process.

Initially, this process began with the introduction of audio and video recording technologies, followed by the integration of computerized systems, the widespread use of Internet technologies, and, in its most recent phase, the establishment of a comprehensive system for handling digital evidence, reaching its highest level of development.

Based on the above-mentioned scientific research and historical analysis, we propose to classify the historical development of the use of electronic evidence at the stage of pre-trial proceedings in the Republic of Uzbekistan into the following main stages of development:

The first stage is the phase of active introduction of electronic data storage media into pre-trial proceedings, covering the period from the independence of the Republic of Uzbekistan up to approximately 1999. During this period, alongside the introduction of electronic computing technologies and magnetic recording devices into criminal procedural activities, the rapid development of information technologies led to the emergence of new methods for working with digitized data in preliminary investigation practice. This stage was significant in determining the role and importance of electronic data and their storage media in criminal proceedings, as electronic technologies began to transform from auxiliary tools into primary sources for the collection of evidence.

The second stage spans from 2000 to the present day. During this period, electronic data and their storage media have evolved from being merely important auxiliary tools in investigations to becoming mandatory requirements for certain procedural actions. A distinctive feature of this stage is that the admissibility criteria of digital evidence have

become a key factor determining the quality and effectiveness of pre-investigation checks, inquiry, and preliminary investigation processes. In this period, failure to document certain investigative actions by means of video recording has led to situations where evidence may lose its procedural admissibility. This stage culminated in the establishment of detailed legal norms in criminal procedural legislation defining such concepts as "electronic data" and "digital evidence," as well as regulating the procedures for their collection, submission, inspection, examination, and evaluation.

4. Conclusion

In conclusion, the emergence and development of the need to use electronic evidence is closely connected with the rapid advancement of information and communication technologies and the corresponding growth of cybercrime. Electronic evidence has evolved from a supplementary tool into a fundamental component of criminal procedural activity.

The historical analysis demonstrates that the formation of electronic evidence passed through several important stages, beginning with the introduction of audio and video recording technologies, followed by the development of computer systems, and culminating in the establishment of digital forensics and comprehensive legal regulation.

In the Republic of Uzbekistan, significant progress has been made in creating a legal framework governing electronic data and digital evidence. Legislative reforms have introduced clear definitions, procedures for collection and evaluation, and requirements ensuring the admissibility and reliability of such evidence.

At the same time, the increasing complexity of digital technologies requires continuous improvement of legal norms, technical capabilities, and professional skills of law enforcement agencies. Ensuring the integrity, authenticity, and proper use of electronic evidence remains a key challenge.

Therefore, further development of this field should focus on strengthening legal regulation, enhancing international cooperation, and improving methodological approaches to the use of electronic evidence in criminal proceedings.

REFERENCES

[1] Address of the President of the Republic of Uzbekistan Shavkat Mirziyoyev at the videoconference meeting of January 19, 2021. – URL: https://president.uz
[2] Levy S. Hackers: Heroes of the Computer Revolution. – New York, 1984.
[3] Thomas J. The History of Computer Viruses. – 2003.
[4] Denning D.E. Information Warfare and Security. – Addison-Wesley, 1999.
[5] Spafford E.H. The Internet Worm Incident // Purdue University Report, 1988.
[6] Casey E. Digital Evidence and Computer Crime. – Elsevier, 2011.
[7] Casey E. Digital Evidence and Computer Crime. – Elsevier, 2004.
[8] Computer Fraud and Abuse Act (CFAA), USA, 1986.
[9] International Journal of Digital Evidence. – 2002. – Vol. 1, Issue 1. – URL: https://www.utica.edu
[10] Criminalistics. Textbook. – Tashkent: Tashkent State University of Law.
[11] Convention on Cybercrime (Budapest Convention). – Council of Europe, 2001.
[12] Sergeev M.S. Legal Regulation of the Use of Electronic Information... – Kazan, 2018.
[13] Decree of the Presidium of the Supreme Soviet of the RSFSR dated August 31, 1966.
[14] Law of the Republic of Uzbekistan dated April 19, 2018. – URL: https://lex.uz
[15] Law of the Republic of Uzbekistan dated May 23, 2019. – URL: https://lex.uz
[16] Law of the Republic of Uzbekistan dated January 12, 2021. – URL: https://lex.uz
[17] Law of the Republic of Uzbekistan dated May 14, 2020. – URL: https://lex.uz
[18] Law of the Republic of Uzbekistan dated November 21, 2024 No. ZRU-1003. – URL: https://lex.uz
[19] Criminal Procedure Code of the Republic of Uzbekistan. – URL: https://lex.uz

[20] Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan dated June 23, 2025.
[21] Resolution No. 24 of the Plenum of the Supreme Court of the Republic of Uzbekistan dated August 24, 2018.