SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

ELECTRONIC EVIDENCE IN CRIMINAL JUSTICE: CHALLENGES OF AUTHENTICITY AND ADMISSIBILITY

Abdieva Dilfuza Ikhtiyorovna
National University of Uzbekistan named after Mirzo Ulugbek
Second-Year Student, Bachelor of Laws (LL.B.), Faculty of Social Sciences
E-mail: abdiyevakookowa@gmail.com | Tel: +998 90 070 65 50

Abstract. This article studies the problems of authenticity and admissibility of electronic evidence in criminal justice. Because digital technology is now used everywhere, electronic data such as emails, social media messages, bank records and video surveillance footage are increasingly used as evidence in criminal cases. However, the special technical nature of this data creates new legal problems that traditional rules of evidence do not fully address. The study uses formal legal, comparative legal and historical legal methods to analyze the rules on electronic evidence in the Criminal Procedure Code of the Republic of Uzbekistan, together with the Law "On Electronic Document Circulation" and the Law "On Cybersecurity". These national rules are compared with the approach used in the United States and the European Union. The analysis shows that Uzbek law does not yet clearly define electronic evidence as an independent type of evidence, and it does not set clear criteria for checking the authenticity of such evidence or for conducting technical forensic examination. The article ends with practical recommendations for improving the law, including a clear legal definition of electronic evidence, mandatory digital forensic examination, use of hash based verification methods, and stronger international cooperation on cross border evidence requests.

Keywords: *electronic evidence, criminal procedure, authenticity of evidence, admissibility of evidence, digital forensics, cybersecurity, judicial practice*

In contemporary criminal procedure, the growing use of digital technology has made electronic information an integral part of criminal case handling. Mobile communication devices, social networks, electronic mail, databases of banking transactions and video surveillance systems increasingly provide material that is used as evidence in practice. At the same time, the specific nature of such information, in particular the ease with which it can be altered, copied or destroyed, raises serious theoretical and practical problems in ensuring its authenticity and procedural admissibility. This situation explains the relevance of the topic, because traditional evidentiary theory and practice were developed mainly for physical and written evidence and do not fully capture the particular features of electronic data.

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor | (2023): 5.913 |
Volume-9, Issue-02, Published | 11-08-2026 |

The legal regulation of electronic evidence in the Republic of Uzbekistan has been developing gradually. In particular, the Criminal Procedure Code of the Republic of Uzbekistan has undergone a number of institutional updates aimed at recognizing electronic data as an independent type of evidence. In addition, the Law "On Electronic Document Circulation" and the Law "On Cybersecurity" serve as a general framework for legal relations arising in the electronic environment. Even so, the existing regulation does not fully address a number of practical questions that arise at the stages of collecting, securing, storing and judicially assessing electronic evidence.

An analysis of the scientific literature on the subject shows that foreign legal scholarship, particularly in the United States, the United Kingdom and the countries of the European Union, has given considerable attention to the problem of electronic evidence, and that these jurisdictions have built comparatively robust procedural mechanisms for verifying its authenticity. In the legal scholarship of the Commonwealth of Independent States and of Uzbekistan, however, the subject remains relatively new, and comprehensive theoretical and applied research is still limited. It is precisely this gap that defines the scientific novelty of the present study, which develops a systemic approach to ensuring the authenticity and admissibility of electronic evidence by comparing Uzbek legislation with foreign practice.

The purpose of the study is to examine the legal and theoretical foundations for ensuring the authenticity and procedural admissibility of electronic evidence in criminal proceedings, to identify shortcomings in national legislation and to develop scientifically grounded proposals for addressing them. To achieve this purpose, the following tasks were set: to clarify the concept and legal nature of electronic evidence; to analyze the norms of the criminal procedure legislation of the Republic of Uzbekistan governing electronic evidence; to conduct a comparative study of foreign practice; to identify the problems that arise in practice; and to formulate proposals for improving the legislation. It is worth noting that the study seeks to analyze electronic evidence not only from a procedural standpoint but also from a technical and forensic one, which allows for a more integrated approach to the subject.

The methodology of the study rests on a combination of general scientific and special legal methods. The formal legal method was used to analyze, in textual terms, the norms of the Criminal Procedure Code of the Republic of Uzbekistan relating to electronic evidence, as well as the relevant provisions of the Law "On Electronic Document Circulation" and the Law "On Cybersecurity". The comparative legal method made it possible to compare the regulatory model adopted in Uzbekistan with the Federal Rules of Evidence of the United States, the regulation of the European Union on electronic identification and trust services known as eIDAS, and the approach to computer evidence developed in the courts of the United Kingdom. The historical legal method was applied to trace the stages in the formation of the institution of

JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

electronic evidence in the criminal procedure legislation of Uzbekistan, including the amendments made to the Criminal Procedure Code, adopted in 1994, in subsequent years. Systemic analysis and logical generalization were also used to evaluate the legal norms in their interrelation, as a coherent whole.

The source base of the study consists of the current legislation of the Republic of Uzbekistan, in particular the Criminal Procedure Code, the Law "On Electronic Document Circulation" and the Law "On Cybersecurity", together with the relevant resolutions of the Plenum of the Supreme Court of the Republic of Uzbekistan. In addition, the texts of legal acts confirmed through the national legal information portal lex.uz, official materials of the Council of Europe on combating cybercrime, and foreign and domestic scholarly literature were used as sources for the analysis. Practical examples are drawn from investigative and judicial practice, as well as from official analytical materials on the subject.

Article 81 of the Criminal Procedure Code of the Republic of Uzbekistan, devoted to the system of evidence, lists the types of evidence recognized in criminal proceedings. Under this provision, the testimony of witnesses, victims, suspects, the accused and defendants, expert opinions, as well as physical and digital evidence, audio and video recordings, and materials consisting of film footage and photographs are all recognized as sources of evidence. This provision creates the procedural possibility of using electronic information as evidence, but the Code does not provide a separate, independent definition of the concept of electronic evidence in its general part, which creates certain difficulties in practice when distinguishing it from other types of evidence.

Chapter 25 of the Code, entitled "Attaching Objects, Documents and Electronic Data to a Case as Physical, Written and Digital Evidence", establishes the procedure for seizing electronic data from physical carriers, storing it and attaching it to a criminal case. Article 105 of the Code sets out the procedure for showing objects, documents and electronic data to the person being questioned, while Article 140 governs the inspection of objects, documents and electronic data. These provisions form the legal basis for procedurally recording electronic information during investigative actions. Articles 91(1) through 91(4) of the Code, in turn, establish the procedure for conducting investigative actions by videoconference, which indirectly broadens the legal basis for procedural actions carried out in an electronic environment.

On the question of admissibility, Article 95(1) of the Code sets out the criteria for the inadmissibility of evidence, establishing in particular that information obtained in violation of legal requirements cannot be admitted as evidence. Together with Resolution No. 24 of the Plenum of the Supreme Court of the Republic of Uzbekistan of 24 August 2018, "On Certain Issues of Application of Criminal Procedure Law Norms Concerning Admissibility of Evidence", this provision creates a general legal

JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

basis for verifying whether electronic evidence has been obtained in accordance with the required procedure. The analysis shows that the existing regulation mainly covers the external procedural side of seizing and attaching electronic data, while the criteria for confirming its technical authenticity, that is, whether the information originates from its claimed source, has not been altered and retains its integrity, are not expressed with sufficient precision at the level of statute.

The Law "On Electronic Document Circulation", adopted on 29 April 2004 under No. 611-II, is closely connected with the subject of electronic evidence and establishes the legal force of electronic documents, their required elements, and the rights and obligations of participants in electronic document circulation. This law creates the general basis for recognizing the legal significance of electronic information by equating a document certified with an electronic digital signature to a paper document, but it is oriented mainly toward civil and administrative relations and does not separately regulate the specific features of using electronic material as evidence in criminal proceedings. The Law "On Cybersecurity" (No. O'RQ-764, 15 April 2022) regulates relations arising from cyber threats, cyberattacks and computer incidents affecting information systems and resources, and thereby extends the institutional basis for identifying and securing electronic evidence in the investigation of cybercrime. The legal force of electronic documents is also closely linked to the new Law "On Electronic Digital Signature" of 12 October 2022 (No. O'RQ-793), which introduces an updated regime governing electronic signature keys and certificates.

Compared with foreign practice, in the legal system of the United States, Rule 901 of the Federal Rules of Evidence sets out the general requirement for authenticating electronic evidence, namely that the party offering the evidence must show that it is what it is claimed to be. Rules 902(13) and 902(14), which came into effect on 1 December 2017, provide a simplified procedure that allows electronic records and copies of them to be recognized as self authenticating on the basis of a certification by a qualified person, without the need for witness testimony in court. In the European Union, Regulation (EU) No 910/2014 of 23 July 2014, known as eIDAS, establishes a single legal status for electronic identification and trust services and ensures the cross border recognition of electronic signatures and electronic seals, which allows electronic evidence to be assessed on the basis of uniform trust criteria among the member states of the European Union. The Council of Europe Convention on Cybercrime, known as the Budapest Convention, has created a mechanism for international cooperation in investigating cybercrime and obtaining electronic evidence across borders. The Republic of Uzbekistan has not yet acceded to this convention, but it takes an active part in efforts to move closer to international standards through regional cooperation, in particular through the Central Asian regional workshop on requesting electronic evidence across borders held in Tashkent

JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

in November 2025 under the initiative of the Organization for Security and Co-operation in Europe.

An analysis of examples drawn from practice shows that in criminal cases involving financial fraud, cybercrime and corruption, banking transaction histories, records of subscriber movement held by mobile network operators, and correspondence from messaging applications are increasingly used as evidence. However, the procedures for seizing such data, conducting technical examinations and forensically confirming its integrity do not yet follow a uniform standard in practice, which creates a risk that different courts may apply different approaches to the same type of evidence.

The results of the analysis reveal a number of theoretical problems concerning the legal nature of electronic evidence. First, because the status of electronic evidence as an independent type of evidence is not fully established in the Code, in practice it is often assessed under the regime applicable to physical or written evidence. In other words, the specific technological features of electronic data, in particular its digital nature, which carries a high risk of copying, remote alteration and destruction, are not sufficiently taken into account within the traditional evidentiary regime. This, in turn, creates a need to develop separate procedural criteria for verifying the authenticity of electronic evidence as a distinct procedural institution.

Second, the law does not sufficiently regulate the participation of specialists with the necessary technical knowledge in seizing electronic evidence and conducting investigative actions. As a result, in some cases the technically incorrect seizure or storage of electronic data may lead a court later to find the evidence inadmissible. Addressing this problem would benefit from special procedural norms establishing a mandatory forensic technical examination.

Third, the cross border collection of electronic evidence presents particular complexity. A large share of modern crime involves data located on foreign servers, at international information technology companies, or in cloud storage services, yet the Republic of Uzbekistan currently has limited formal international legal mechanisms for obtaining such data promptly from foreign jurisdictions. Foreign practice, in particular the approaches taken in the United States and the European Union based on expedited preservation and trusted third party institutions, could serve as a useful methodological reference for addressing this gap.

As a further problem, the study found that judges and investigative officers often lack sufficient specialized technical training to assess electronic evidence. This increases the risk of an unclear or incorrect legal assessment of such evidence, because the technical authenticity of evidence is often assessed solely on the basis of an expert opinion, and courts do not always have the capacity to verify such an opinion independently.

JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

Based on the foregoing, the following conclusions can be drawn. Although the current criminal procedure legislation of the Republic of Uzbekistan has created a general procedural basis for admitting electronic information as evidence, the independent legal status of electronic evidence, the criteria for confirming its authenticity, and the procedures for technical forensic examination are not established with sufficient clarity and system at the level of statute. This, in turn, may lead to inconsistency in law enforcement practice and to an increase in disputes over the procedural admissibility of electronic evidence.

With a view to improving the legislation, the following specific proposals are put forward. First, an independent statutory definition of the concept of electronic evidence should be introduced into the chapters of the Criminal Procedure Code devoted to evidence, clearly setting out the criteria for confirming the source, integrity and unaltered condition of electronic data. Second, procedural norms should be introduced requiring the mandatory participation of a specialized forensic technical expert in seizing, copying and storing electronic evidence, in line with the digital forensics standards developed in the practice of the United States and the European Union. Third, it is recommended that the use of hash values and other cryptographic methods to technically confirm the integrity of electronic evidence be established as a mandatory procedural requirement, which would make it possible to objectively confirm that evidence has not been altered during court proceedings. Fourth, introducing specialized training programs on working with electronic evidence for judges, investigators and prosecutors would help raise their level of technical competence. Fifth, it would be advisable to expand international cooperation on obtaining electronic evidence across borders, including a comprehensive study of the possibility of joining the relevant international legal mechanisms and making more active use of regional cooperation formats.

In conclusion, it should be emphasized that ensuring the authenticity and admissibility of electronic evidence is not only a legal but also a technological problem, and its effective resolution requires an integrated, interdisciplinary approach combining legal scholarship and information technology. The recommendations proposed in this study may serve as a practical basis for improving the efficiency of criminal proceedings in the Republic of Uzbekistan, for creating additional guarantees for the protection of individual rights and freedoms, and for bringing national legislation closer to international standards.

REFERENCES

1. Criminal Procedure Code of the Republic of Uzbekistan (1994, current edition). National Legal Information Portal. https://lex.uz/docs/-111460

JOURNAL OF LAW AND ECONOMICS
ISSN(Online): 2984-8091
SJIF Impact Factor |(2023): 5.913|
Volume-9, Issue-02, Published |11-08-2026|

2. Law of the Republic of Uzbekistan 'On Electronic Document Circulation', No. 611-II, 29 April 2004. National Legal Information Portal. https://lex.uz/docs/-165079
3. Law of the Republic of Uzbekistan 'On Cybersecurity', No. O'RQ-764, 15 April 2022. National Legal Information Portal. https://lex.uz/uz/docs/-5960604
4. Law of the Republic of Uzbekistan 'On Electronic Digital Signature', No. O'RQ-793, 12 October 2022. National Legal Information Portal. https://lex.uz/docs/-64467
5. Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan No. 24, 24 August 2018, 'On Certain Issues of Application of Criminal Procedure Law Norms Concerning Admissibility of Evidence'.
6. Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan No. 07, 23 May 2014, 'On the Court Verdict'.
7. Council of Europe (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. Strasbourg.
8. Council of Europe (2024). Budapest Convention reaches 75 Parties. Strasbourg: Cybercrime Programme Office.
9. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
10. Federal Judicial Center (2017). Amendments to the Federal Rules of Practice and Procedure: Evidence 2017, Self-Authenticating Electronic Evidence. Washington, D.C.
11. United States Federal Rules of Evidence, Rule 901 and Rule 902(13) and 902(14), amendments effective 1 December 2017.
12. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
13. Fomina, T. H., & Rachynskyi, O. O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. Bulletin of Kharkiv National University of Internal Affairs, 102(3), 207-220. https://doi.org/10.32631/v.2023.3.43