ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS IN RESPUBLIC OF UZBEKISTAN: CRITERIA OF ADMISSIBILITY AND PROBLEMS OF VERIFICATION

Eshkuvatova Diyora Uzok kizi
Master's student of Tashkent State University of Law

Abstract: *This article examines the legal framework and practical challenges of utilizing electronic evidence in the criminal proceedings of the Republic of Uzbekistan. It focuses on the reforms introduced by Law No. ZRU-1003 of November 21, 2024, which formally defined "electronic data" and "digital evidence" and established strict admissibility criteria, including the mandatory participation of specialists and the preservation of data integrity. The study highlights significant verification problems, such as the volatility of digital environments, metadata loss, and the lack of standardized hashing protocols. Additionally, it reviews the latest 2025 Supreme Court Plenary guidance and discusses the prospects for harmonizing national legislation with international standards to ensure effective justice in the digital age.*

Keywords: *electronic evidence, digital evidence, admissibility criteria, criminal proceedings, Uzbekistan, digital forensics, verification problems.*

O'ZBEKISTON RESPUBLIKASI JINOYAT PROTSESSIDA ELEKTRON DALILLAR: MAQBULLIK MEZONLARI VA VERIFIKATSIYA MUAMMOLARI

Eshquvatova Diyora Uzoq qizi
Toshkent davlat yuridik universiteti magistranti

Annotatsiya: *Ushbu maqolada O'zbekiston Respublikasi jinoyat protsessida elektron dalillardan foydalanishning huquqiy asoslari va amaliy muammolari tahlil qilinadi. Tadqiqotda 2024-yil 21-noyabrdagi O'RQ-1003-sonli Qonun bilan kiritilgan yangiliklar, jumladan, «elektron ma'lumotlar» va «raqamli dalillar» tushunchalarining qonuniy mustahkamlanishi hamda ularning maqbullik mezonlari (mutaxassis ishtiroki, butunlikni ta'minlash) ko'rib chiqiladi. Shuningdek, raqamli ma'lumotlarning o'zgaruvchanligi (volatility), metadata yo'qolishi va xeshlash protokollarining yetishmasligi kabi tekshirish (verifikatsiya) jarayonidagi muammolar yoritilgan. Maqolada Oliy sud Plenumining 2025-yildagi so'nggi qarorlari va milliy qonunchilikni xalqaro standartlar bilan uyg'unlashtirish istiqbollari bayon etilgan.*

Kalit so'zlar: *elektron dalillar, raqamli dalillar, maqbullik mezonlari, jinoyat protsessi, O'zbekiston, raqamli kriminalistika, verifikatsiya muammolari.*

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ РЕСПУБЛИКИ УЗБЕКИСТАН: КРИТЕРИИ ДОПУСТИМОСТИ И ПРОБЛЕМЫ ВЕРИФИКАЦИИ

Эшкуватова Диёра Узок кизи
Магистрант Ташкентского государственного юридического университета

Аннотация: *В данной статье анализируются правовые основы и практические проблемы использования электронных доказательств в уголовном процессе Республики Узбекистан. В центре внимания находятся нововведения, внесенные Законом № ЗРУ-1003 от 21 ноября 2024 года, который официально закрепил понятия «электронные данные» и «цифровые доказательства», а также установил строгие критерии их допустимости (обязательное участие специалиста, сохранение целостности). Рассматриваются технические и процедурные сложности верификации, такие как волатильность цифровой среды, потеря метаданных и отсутствие единых стандартов хеширования. В статье также изучены последние разъяснения Пленума Верховного суда 2025 года и вопросы гармонизации национального права с международными стандартами в сфере цифровой криминалистики.*

Ключевые слова: *электронные доказательства, цифровые доказательства, допустимость доказательств, уголовный процесс, Узбекистан, цифровая криминалистика, проблемы верификации.*

The pervasive integration of digital technologies into daily life has driven a structural transformation in the nature of criminal activity within the Republic of Uzbekistan, creating an acute need for a robust digital forensic framework. Statistical indicators illustrate the magnitude of this shift, with offenses committed through information technologies accounting for 44.4 percent of total crime in 2024, before rising to 47.7 percent during the first eleven months of 2025[62]. This surge in cyber-facilitated crime spans approximately 64 distinct categories of offenses within the Criminal Code of the Republic of Uzbekistan, ranging from sophisticated network intrusions to traditional crimes executed via online communication channels[63]. Confronted with this cybercrime wave, traditional law enforcement methodologies have proven increasingly inadequate, prompting a systematic overhaul of the nation's evidentiary rules[64].

This rapid virtualization of criminal activity has forced a paradigm shift in contemporary criminalistics, where the focus of evidence collection must transition from physical, tangible traces to highly volatile digital footprints. To establish the material truth in criminal proceedings, law enforcement agencies must systematically gather, verify, and evaluate electronic records, such as messaging logs, IP addresses, transaction records, and network activity databases[65]. These digital traces possess unique physical and conceptual characteristics, such as ease of modification, susceptibility to remote

[62]The American Journals. (2025). Cybercrime statistics and the digital transformation of criminal activity in Uzbekistan. The American Journal of Political Science, Law, and Criminology, 7(12), 256-265.
[63] The American Journals. (2025). Cybercrime statistics and the digital transformation of criminal activity in Uzbekistan. The American Journal of Political Science, Law, and Criminology, 7(12), 256-265.
[64] Neliti. (2026). The emergence and historical development of electronic evidence in criminal proceedings in Uzbekistan. Neliti Legal Studies Journal, 12(1), 1-15.
[65] RACO. (2024). Challenges in the use of digital evidence in pretrial investigations. Internet, Derecho y Política, 41, 208-212.

deletion, and reliance on specific storage hardware, which distinguish them from conventional material evidence[66]. Consequently, the development of specialized legal standards and technical verification protocols has become a primary requirement for securing the integrity of the judicial process.

Historically, the procedural use of electronic evidence in Uzbekistan evolved through two primary stages, reflecting the gradual maturation of both technological penetration and legal doctrine. The first stage, spanning from national independence in 1991 to approximately 1999, was characterized by the initial introduction of computer systems and magnetic recording devices into the administrative and investigative operations of law enforcement agencies. During this early phase, digitized data was treated as an optional, auxiliary resource rather than an independent source of proof, and the legal framework lacked any specialized protocols for electronic data preservation. While investigative practices slowly adjusted to the presence of digitized accounting records and computer files, the physical medium itself was typically seized under traditional rules governing physical documents, neglecting the unique properties of virtual data.

The second historical stage, beginning in 2000 and continuing to the present day, is marked by a transition where electronic data progressed from an auxiliary investigative resource to a mandatory procedural requirement for specific investigative actions. During this era, the admissibility criteria for digital evidence became a core factor in determining the quality and legality of pre-trial investigations. Under modern regulations, a failure to properly capture and document critical investigative events using digital recording systems can lead directly to the exclusion of the gathered evidence, illustrating how digital recording has become central to procedural legality. This shift culminated in the development of detailed statutory amendments designed to define and regulate digital evidence as an independent legal category.

Date of Enactment	Legislative Instrument	Key Procedural Reforms and Impact on Evidence Lifecycle
May 14, 2020	Law of the Republic of Uzbekistan	Mandated compulsory video recording for critical investigative actions in serious crimes under CPC Article 91.[2]
January 12, 2021	Law of the Republic of Uzbekistan	Introduced CPC Articles 91-1/391-1; established legal framework for videoconferencing and remote digital collection.[2]
July 5, 2021	Presidential Decree No. PF-6256	Formally introduced “electronic evidence” concept; mandated digital forensic research between 2021 and 2025.

[66] App-Journal, 2025

November 30, 2023	Presidential Resolution No. PQ-381	Approved Roadmap requiring formal statutory definitions of electronic data and digital evidence.
November 21, 2024	Law No. ZRU-1003	Codified definitions of electronic data and digital evidence across Criminal, Civil, and Economic Procedure Codes.

The first official mention of “electronic evidence” in Uzbekistan’s legal framework occurred under Presidential Decree No. PF-6256, dated July 5, 2021, which focused on modernizing the forensic examination system[67]. This decree mandated the introduction of specialized forensic examinations and scientific research specifically dedicated to electronic evidence between 2021 and 2025, driving the professionalization of local digital forensics[68]. Following this directive, the "Roadmap" approved by Presidential Resolution No. PQ-381 on November 30, 2023, formally tasked legislative authorities with establishing precise definitions for “electronic data” and “digital evidence”. These policy directives laid the groundwork for aligning national criminal procedures with contemporary international forensic standards[69].

Prior to these comprehensive definitions, incremental changes to the Criminal Procedure Code of the Republic of Uzbekistan established a baseline for digital evidence utilization. The Law of the Republic of Uzbekistan dated May 14, 2020, amended Article 91 of the Criminal Procedure Code to mandate the compulsory use of video recording during critical investigative actions in cases involving especially serious crimes. Under these provisions, actions such as crime scene inspections, searches, seizures, investigative experiments, and detentions must be recorded via video to protect citizen rights. In modern judicial practice, a failure to document these specific actions with video recording represents a serious procedural violation that can cause the collected evidence to lose its admissibility.

Further structures for remote and electronic coordination were established under the Law of the Republic of Uzbekistan dated January 12, 2021, which introduced Articles 91-1 and 391-1 to the Criminal Procedure Code[70]. This legislation created the formal legal basis for the remote collection of electronic data, its digital storage, and its formal procedural documentation using videoconferencing systems during pre-investigation checks and preliminary inquiries. Additionally, this law introduced standardized guidelines for using audio recordings during criminal trials, ensuring that electronic media could be integrated into the official case record. These adjustments reflected an increasing awareness that physical presence was no longer a prerequisite for conducting lawful and effective procedural actions in a digitized society[71].

[67]Neliti. (2026). The emergence and historical development of electronic evidence in criminal proceedings in Uzbekistan. Neliti Legal Studies Journal, 12(1), 1-15.
[68] Neliti. (2026). The emergence and historical development of electronic evidence in criminal proceedings in Uzbekistan. Neliti Legal Studies Journal, 12(1), 1-15.
[69] See in the same place
[70] See in the same place
[71] Gulchehra Tulaganova. (2024). Issues of improvement of the institution of advocacy in criminal proceedings. International Journal of Business, Law, and Political Sciences, 1(9), 112-125.

A legislative milestone was achieved on November 21, 2024, when President Shavkat Mirziyoyev signed a comprehensive law specifically designed to formalize the use of digital evidence in all legal proceedings[72]. Registered as Law No. ZRU-1003, this document had previously faced significant legislative resistance, being rejected twice by deputies in June 2022 and November 2023 due to concerns regarding privacy protections and procedural clarity[73]. Following extensive revisions, the law passed its third reading in the Legislative Chamber on August 27, 2024, received Senate approval on October 24, 2024, and was officially published on Lex.uz[74]. The law's preamble explicitly links its passage to the necessity of establishing clear legal frameworks to counteract the widespread occurrence of crimes in the digital sphere[75].

The systemic impact of Law No. ZRU-1003 is reflected in its broad scope, which introduced amendments to the Criminal Procedure Code, the Civil Procedure Code, the Economic Procedure Code, and the Code of Administrative Responsibility. Corresponding changes were also enacted in national laws governing notarial activities, arbitration courts, and judicial expertise to ensure a unified approach to digital forensics across all legal sectors. This multi-sectoral harmonization ensures that public authorities, private organizations, and defense counsels operate under identical legal definitions and procedural expectations when handling digital traces[76]. By standardizing these rules, the state sought to elevate the credibility of its judicial processes and improve its standing in international legal rankings[77].

Under the amendments introduced by Law No. ZRU-1003, the Criminal Procedure Code now draws a sharp distinction between "electronic data" and "digital evidence." Under Article 89-1 and Article 204-1, electronic data is defined as any information created, processed, and stored utilizing electronic devices, information systems, and information technologies. This definition is intentionally broad, designed to encompass any form of digitized information regardless of its specific format, platform, or transmission protocol. The law permits any participant in a case, including witnesses, victims, suspects, and defendants, to submit electronic data by transferring it from one electronic medium to another, thereby democratizing the process of submitting digital material.

Conversely, "digital evidence" is defined under Article 89-2 and Article 204-2 as electronic data that contains information directly relevant to the facts and circumstances of a case. This category explicitly includes electronic files, audio and video recordings, information extracted from the internet, network activity logs, and other digital footprints used to establish key facts. By establishing this distinction, the law separates raw electronic data from data that has acquired procedural relevance through

[72] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[73] Law on digital evidence adopted in Uzbekistan (2026) – https://www.gazeta.uz/en/2024/11/27/digital-evidence/
[74] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[75] Law on digital evidence adopted in Uzbekistan (2026) – https://www.gazeta.uz/en/2024/11/27/digital-evidence/
[76] Gulchehra Tulaganova. (2024). Issues of improvement of the institution of advocacy in criminal proceedings. International Journal of Business, Law, and Political Sciences, 1(9), 112-125.
[77] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.

its capacity to prove or disprove specific circumstances under investigation[78]. This conceptual separation is crucial for preventing the indiscriminate seizure of digital data that has no bearing on the criminal inquiry.

During the legislative drafting process, lawmakers drew a distinction between the procedural obligations in civil and economic cases versus those in criminal proceedings. In civil and economic disputes, parties are strictly required to submit digital evidence along with the physical storage device, and must formally notify the court with an explanation if they are unable to do so[79]. A similar obligation was initially proposed for criminal cases but was ultimately excluded during the legislative review in the Legislative Chamber. This deliberate exclusion recognizes the unequal power dynamics in criminal investigations, ensuring that defendants and witnesses are not unduly burdened with presenting original hardware when copies can be verified through forensic channels.

Legal Dimension	Criminal Proceedings (CPC)	Civil and Economic Proceedings (CPC / EPC)
Submission of Physical Medium	Not mandatory; copy-based submission permitted to protect defense from undue burdens.[5]	Mandatory; parties must submit original physical medium or formally explain the omission.[5]
Paper-Printed Copies	Allowed as submissions but cannot be regarded as written evidence under the CPC.[6]	Allowed as valid written evidence provided they are formally notarized.[5]
Specialist Participation	Mandatory; any data obtained during search or seizure without a specialist is inadmissible.[5]	Regulated under general rules; specialist involvement is not an absolute bar to admissibility.[6]
Seizure Authorization	Strictly requires prior court authorization and a legal warrant for personal electronic data.[5]	Governed by general civil discovery rules and party-driven evidence production.[5]

The law also establishes strict parameters regarding the validity of paper-printed copies of digital evidence. While participants in criminal proceedings are permitted to submit printed copies of digital data, such paper forms can never be regarded as written evidence under the Criminal Procedure Code. This stands in contrast to civil and economic proceedings, where paper copies are legally valid as written evidence provided they have been officially notarized. This procedural divergence highlights the higher standard of proof required in criminal matters, where the risk of document manipulation or loss of metadata during printing makes paper representations inherently unreliable for establishing criminal guilt[80].

The most critical admissibility criterion introduced by Law No. ZRU-1003 is the "Specialist Rule," which governs the collection and review of all digital material. The law

[78] App-Journal. (2025). The legal nature and verification challenges of digital evidence in criminal proceedings. Applied Journal of Forensic Sciences, 48(2), 42-53.
[79] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[80] App-Journal. (2025). The legal nature and verification challenges of digital evidence in criminal proceedings. Applied Journal of Forensic Sciences, 48(2), 42-53.

dictates that submitted electronic data must be reviewed by the investigating officer, investigator, prosecutor, or court strictly in the presence of a technical specialist, and only after examining the original medium containing the data. To enforce compliance, the legislature enacted a strict inadmissibility rule: any electronic data obtained during investigative procedures without the direct involvement of a specialist is deemed legally inadmissible[81]. This rule serves as a procedural shield, protecting against the manipulation, corruption, or improper handling of volatile data by non-technical law enforcement officers[82].

This mandatory specialist involvement fundamentally changes how law enforcement must execute search and seizure operations involving electronic devices. Historically, investigators could seize computers, smartphones, and hard drives without immediate technical oversight, often leading to the alteration of system files or the destruction of temporary memory during transport[83]. Under the current regime, the absence of a qualified digital forensic specialist at the scene of data acquisition creates a fatal procedural defect that cannot be cured at a later stage of the proceedings[84]. This structural constraint forces investigative organs to coordinate closely with certified forensic laboratories and specialized technical units during the critical initial phases of an investigation[85].

Further safeguards require that the integrity and authenticity of digital evidence must be fully ensured during any transfer or copying process between devices[86]. Under Article 89-2, copies of digital evidence are admissible in court only if the original media from which they were extracted are available for verification, unless the digital evidence has been formally certified by a notary. This requirement addresses the core vulnerability of digital files—their susceptibility to undetectable modification—by requiring a continuous, verifiable link back to the primary source of the data. If the original physical medium is destroyed or unavailable, and no notarized certification exists, any copied data loses its admissibility, protecting the accused from potentially falsified digital materials.

Constitutional protections regarding privacy and personal data are also integrated into the new digital evidence framework. Law No. ZRU-1003 stipulates that searches and seizures of personal electronic data can only be conducted on the basis of the law and with explicit court authorization. This judicial warrant requirement aligns digital searches with traditional protections against unlawful interference with a citizen's private life and correspondence. By requiring prior judicial review, the law prevents fishing expeditions by law enforcement agencies and ensures that the collection of digital data is proportional to the gravity of the offense being investigated[87].

To prevent the unnecessary retention of personal information, the law mandates the prompt return of irrelevant hardware. Under Article 89-1, any electronic media seized

[81] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[82] Zenodo. (2026). Contemporary problems of collecting and recording digital evidence in criminal proceedings. Zenodo Open Archive.
[83] See in the same place
[84] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[85] UNODC. (2025). Improving forensic capacities in Uzbekistan – Phase III. Tashkent: UNODC Regional Office for Central Asia.
[86] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[87] RACO. (2024). Challenges in the use of digital evidence in pretrial investigations. Internet, Derecho y Política, 41, 208-212.

during an investigation that contains data deemed irrelevant to the case must be returned to its rightful owner without delay. This rule is designed to minimize the disruption caused to citizens and organizations when their smartphones, computers, or storage devices are impounded during criminal inquiries[88]. It also restricts the state's capacity to hoard non-evidence-related personal data, establishing a clear statutory boundary between legitimate evidence collection and arbitrary state surveillance[89].

Following the enactment of Law No. ZRU-1003, the judiciary moved quickly to integrate these statutory rules into operational court practices. On June 23, 2025, the Plenum of the Supreme Court of the Republic of Uzbekistan issued Plenary Resolution No. 14, amending its landmark 2018 resolution, Resolution No. 24, which governs the admissibility of evidence. This resolution formally updated the judicial terminology, systematically replacing the general term "evidence" with the phrase "physical and digital evidence" across key directives. It also expanded Point 9 of the original resolution to include "electronic" inspections within the scope of recognized judicial examinations, signaling to lower courts that digital verification must be treated with the same procedural rigor as physical evidence[90].

Plenary Resolution No. 14 established detailed, non-negotiable conditions for the admissibility of digital materials submitted alongside crime reports. Under the completely revised Point 10, documents, electronic data, photographs, and audio or video recordings submitted voluntarily by citizens or organizations can only be deemed admissible if the individuals who presented them are subsequently interrogated. This interrogation must formally establish who found the data, when and where it was discovered, under what specific circumstances it was obtained, or how the recording was made[91]. This requirement effectively eliminates anonymous or unverified digital submissions from being used as key evidence, ensuring that every digital trace can be traced back to a human source who can be cross-examined[92].

Furthermore, the Plenum of the Supreme Court clarified the strict procedural order required for attaching electronic data to a criminal case file. For submitted electronic items to be formally recognized as admissible physical, written, or digital evidence, the prosecuting authority or court must issue a formal ruling strictly after compiling the protocol of their inspection. This rule prevents investigators from pre-emptively designating electronic data as evidence before its contents and origins have been formally examined and documented in an official protocol. In cases of technical ambiguity, the resolution authorizes judicial officers to order a formal forensic examination to resolve whether the electronic data should be attached to the case, reinforcing the role of scientific analysis in judicial decision-making.

[88] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[89] See in the same place
[90] Plenum of the Supreme Court of the Republic of Uzbekistan. (2025). Resolution No. 14: On making amendments and additions to Resolution No. 24 of August 24, 2018, regarding the admissibility of evidence. Lex.uz.
[91] See in the same place
[92] App-Journal. (2025). The legal nature and verification challenges of digital evidence in criminal proceedings. Applied Journal of Forensic Sciences, 48(2), 42-53.

Despite these robust legislative and judicial frameworks, the practical verification of digital evidence in Uzbekistan faces significant technological and procedural obstacles. The high volatility of digital environments remains a primary risk, as data can be easily altered, corrupted, or completely erased during the critical moment of seizure or transfer between devices. Because digital information exists in a virtual, transient state, even minor technical errors during the extraction process can permanently change the metadata or file structure[93]. This technical fragility makes it exceptionally difficult for investigators to prove to a court that the evidence presented is an exact, unaltered replica of the data found at the scene[94].

A critical vulnerability in Uzbekistan's current digital forensic practice is the loss of metadata due to incomplete documentation during the acquisition process. Metadata, which includes timestamps, author details, and file history, is vital for establishing the authenticity of a file, yet it is often discarded when investigators perform simple file copies rather than bit-stream forensic images. Furthermore, there is a distinct lack of comprehensive local regulation regarding hashing—the mathematical algorithm used to generate a unique digital fingerprint for verifying that a file has not been modified. Without standardized hashing protocols mandated by law, the integrity of digital evidence can be easily challenged by defense attorneys, undermining the credibility of the prosecution's case.

The proliferation of encrypted, synchronized, and cloud-based communication devices introduces further complexity to the verification process. Modern smartphones and computers are frequently secured with advanced encryption standards that law enforcement agencies lack the technical capacity to bypass without the cooperation of the user. Moreover, because cloud synchronization continuously updates files across multiple devices, data can be altered remotely even after a physical device has been seized and placed in storage. This active synchronization complicates the task of proving that the data was not tampered with post-seizure, demanding sophisticated signal-blocking storage solutions that are not yet universally available to regional investigative units in Uzbekistan[95].

The verification of digital evidence is also hindered by the absence of localized forensic tool-validation frameworks. Forensic software used to extract and analyze data from electronic devices must be scientifically proven to be accurate and reliable, yet Uzbekistan currently lacks a formal national mechanism to validate these tools. This lack of standardized validation means that different law enforcement agencies may use uncertified or outdated software, creating a risk that extraction errors could occur. To resolve this, digital forensic experts argue that the trustworthiness of digital proof must rely on a repeatable, transparent, and legally authorized procedure rather than the mere existence of the data itself.

[93] Zenodo. (2026). Contemporary problems of collecting and recording digital evidence in criminal proceedings. Zenodo Open Archive.
[94] App-Journal. (2025). The legal nature and verification challenges of digital evidence in criminal proceedings. Applied Journal of Forensic Sciences, 48(2), 42-53.
[95] UNODC. (2025). Improving forensic capacities in Uzbekistan – Phase III. Tashkent: UNODC Regional Office for Central Asia.

Maintaining a secure digital chain of custody represents a persistent organizational barrier within the Uzbekistani justice system. Traditional chain of custody protocols, designed for tangible physical items like weapons or paper documents, are ill-suited for tracking the complex, non-physical history of digital files[96]. A digital chain of custody requires detailed logs showing every individual who accessed, copied, or analyzed the digital file, alongside corresponding hash values at each transfer stage. The absence of automated, standardized digital tracking systems across regional police departments leads to gaps in documentation, leaving room for allegations of unauthorized access or evidence tampering[97].

These digital forensic challenges are situated within a broader, ongoing modernization of the Uzbekistani judiciary initiated under President Shavkat Mirziyoyev's administration. Beginning with the "Five-Point Development Strategy Plan for 2017-2021," the state enacted extensive reforms focusing on court specialization, the creation of a Supreme Judicial Council, and the establishment of new judicial tenure rules to secure independence. The judiciary also introduced automated case assignment systems and electronic filing platforms to improve transparency and reduce corruption. This structural transformation of the justice sector provided the institutional stability necessary to support complex legislative reforms like the 2024 digital evidence amendments[98].

To address the acute shortage of specialized technical expertise, Uzbekistan has invested in targeted scientific and educational institutions. A key development was the establishment of the Scientific and Research Institute of Digital Forensics within the Law Enforcement Academy of the Republic of Uzbekistan, led by forensic expert Gayrat Musaev. This institute plays a central role in conducting high-level digital research, developing specialized forensic methodologies, and training judicial and law enforcement personnel[99]. By consolidating digital forensic expertise within a dedicated academic institution, the state aims to bridge the gap between rapidly evolving technology and judicial practice, ensuring that judges and investigators are equipped to handle complex digital traces[100].

Forensic modernization has also been bolstered by close cooperation with international development partners, such as the United Nations Office on Drugs and Crime (UNODC). Under the "Improving Forensic Capacities in Uzbekistan" project, funded by the US State Department's Bureau of International Narcotics and Law Enforcement Affairs, leading forensic experts have formulated comprehensive strategies to upgrade crime scene evidence management. These strategies emphasize the development of intensive training courses for prosecutors and investigators covering digital forensics, the creation of standardized national training modules, and the establishment of Uniform

[96] App-Journal. (2025). The legal nature and verification challenges of digital evidence in criminal proceedings. Applied Journal of Forensic Sciences, 48(2), 42-53.
[97] RACO. (2024). Challenges in the use of digital evidence in pretrial investigations. Internet, Derecho y Política, 41, 208-212.
[98] Kun.uz. (2024). Uzbekistan adopts landmark law on digital evidence. Kun.uz News Agency.
[99] OSCE. (2024). OSCE builds Uzbekistan's capacity in requesting electronic evidence across borders. OSCE Secretariat.
[100] Neliti. (2026). The emergence and historical development of electronic evidence in criminal proceedings in Uzbekistan. Neliti Legal Studies Journal, 12(1), 1-15.

Coordination Protocols. Furthermore, the project has facilitated direct investment in cutting-edge forensic equipment and digital recording systems for regional law enforcement units[101].

The cross-border nature of digital data represents a major jurisdictional challenge for Uzbekistani investigators, as cloud data is frequently stored on servers located in foreign countries. To address this, the Transnational Threats Department of the Organization for Security and Co-operation in Europe (OSCE) has actively built Uzbekistan's capacity to request electronic evidence across borders. Under Project E-VIDENCE, supported by Germany and the Netherlands, international experts conducted a detailed needs assessment in July 2024 to identify legal and procedural gaps in Uzbekistan's cross-border cooperation framework.

This project aims to establish standardized operating procedures that allow Uzbekistani authorities to obtain data from foreign service providers while strictly respecting international human rights and privacy standards[102].

To streamline the operational handling of these international requests, the Prosecutor General's Office (PGO) of Uzbekistan has received significant technological upgrades.

Through the "Digitalization of International Legal Cooperation Processes" project, implemented by the UNODC, the PGO was equipped with advanced hardware and secure communication platforms designed to handle Mutual Legal Assistance (MLA) cases.

This digital infrastructure accelerates the processing of cross-border evidence requests, allowing investigators to track international cases more effectively and coordinate structured data exchanges with foreign jurisdictions.

This modernized communication network is vital for ensuring that electronic evidence stored abroad can be secured before it is deleted or altered by foreign service providers[103].

Uzbekistan's strategic alignment with global cyber-security frameworks culminated in its active participation in international treaty regimes. In late October 2024, Uzbekistan formally signed the new United Nations Convention Against Cybercrime, which establishes global standards for the preservation of digital evidence and rapid international cooperation.

Additionally, during the Central Asian Regional Workshop held in Tashkent in November 2024, state representatives announced that Uzbekistan would officially initiate the process of joining the Budapest Convention on Cybercrime.

By acceding to these major international treaties, Uzbekistan commits to harmonizing its domestic laws with global standards, ensuring that its digital evidence procedures protect privacy and adhere to the rule of law while combating transnational cybercrime[104].

[101] UNODC. (2025). Improving forensic capacities in Uzbekistan – Phase III. Tashkent: UNODC Regional Office for Central Asia.
[102] OSCE. (2024). OSCE builds Uzbekistan's capacity in requesting electronic evidence across borders. OSCE Secretariat.
[103] UNODC. (2025). Improving forensic capacities in Uzbekistan – Phase III. Tashkent: UNODC Regional Office for Central Asia.
[104] OSCE. (2024). OSCE builds Uzbekistan's capacity in requesting electronic evidence across borders. OSCE Secretariat.

REFERENCES:

1. Social Need for Digitization of Criminal-Procedural Legislation https://www.theamericanjournals.com/index.php/tajpslc/article/download/7830/7142/11681

2. The Emergence and Historical Development of the Need to use Electronic Evidence - Neliti https://media.neliti.com/media/publications/703443-the-emergence-and-historical-development-70968e98.pdf

3. Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international prac - RACO, https://raco.cat/index.php/IDP/article/view/433072/538931

4. DIGITAL EVIDENCES IN CRIMINAL PROCEEDINGS: PROBLEMS OF AUTHENTICITY AND ADMISSIBILITY, https://app-journal.in.ua/wp-content/uploads/2025/10/48-2.pdf

5. Uzbekistan adopts landmark law on digital evidence - Kun.uz, https://kun.uz/en/84589890?utm_source=chatgpt.com

6. Law on digital evidence adopted in Uzbekistan (2026)– https://www.gazeta.uz/en/2024/11/27/digital-evidence/

7. Volume 1 Nomor 9 September 2024 ISSUES OF IMPROVEMENT OF THE INSTITUTION OF ADVOCACY IN CRIMINAL PROCEEDINGS Gulchehra Tulaganov - Antis Publisher, https://e-journal.antispublisher.id/index.php/IJBLPS/article/view/189/156

8. В Узбекистане подписан закон о цифровых доказательствах - Gazeta.uz, https://www.gazeta.uz/ru/2024/11/26/digital-evidence/

9. Закон о цифровых доказательствах подписан президентом. Главное - Spot.uz, https://www.spot.uz/ru/2024/11/22/digital-evidence/

10. ЗРУ-1003-сон 21.11.2024. О внесении изменений и дополнений ..., https://lex.uz/docs/7228823?ONDATE=21.11.2024%2000

11. PROBLEMS OF COLLECTING AND PRESERVING DIGITAL ..., https://zenodo.org/records/19914535

12. Uzbekistan Boosts Forensic Capabilities: National Experts Forger Path for Enhanced Crime Scene Evidence Management - Unodc, https://www.unodc.org/roca/en/NEWS/2025/uzbekistan-boosts-forensic-capabilities-national-experts-forger-path-for-enhanced-crime-scene-evidence-management.html

13. Criminal procedure code of the republic of uzbekistan - Police and Human Rights Resources, https://policehumanrightsresources.org/content/uploads/2016/07/Criminal-Procedure-Law-Uzbekistan-1994.pdf?x36399

14. Criminal Procedure Code of the Republic of Uzbekistan (1994, as amended 2001) (excerpts related to Fair Trial (Right to a)) (English) | LEGISLATIONLINE, https://legislationline.org/taxonomy/term/23015

15. Постановление Пленума Верховного суда Республики Узбекистан от 23.06.2025 г. N 14 "О внесении изменений и дополнений в постановление Пленума Верховного суда Республики Узбекистан от 24 августа 2018 года N 24 "О некоторых вопросах применения норм уголовно-процессуального закона о допустимости доказательств" | Изменения и дополнения в постановления Пленума ВС РУз | Постановления Пленума Верховного суда | Судебные акты - NRM.uz, https://nrm.uz/contentf?doc=784226_postanovlenie_plenuma_verhovnogo_suda_respubliki_uzbekistan_ot_23_06_2025_g_n_14_o_vnesenii_izmeneniy_i_dopolneniy_v_postanovlenie_plenuma_verhovnogo_suda_respubliki_uzbekistan_ot_24_avgusta_2018_goda_n_24_o_nekotoryh_voprosah_primeneniya_norm_ugolovno-processualnogo_zakona_o_dopustimosti_dokazatelstv&products=1_vse_zakonodatelstvo_uzbekistana

16. www.lex.uz, https://www.lex.uz/acts/7613629

17. Digital Traces as an Object of Forensic Research: Concept, Classification and Evidentiary Challenges - IRSHAD JOURNALS, https://irshadjournals.com/index.php/ujldp/article/view/470

18. Legal Reforms in Uzbekistan: A New Era | Federal Judicial Center, https://www.fjc.gov/content/351047/legal-reforms-uzbekistan-new-era

19. Uzbekistan | Judiciaries Worldwide - Federal Judicial Center |, http://judiciariesworldwide.fjc.gov/country-profile/uzbekistan

20. OSCE builds Uzbekistan's capacity in requesting electronic evidence across borders, https://www.osce.org/secretariat/583204

21. Central Asian countries strengthen regional co-operation on electronic evidence - OSCE.org, https://www.osce.org/secretariat/601158

22. Strengthening Uzbekistan's Capacity for Cross-Border Justice: Digitalization Project Delivers New IT Equipment to the PGO - Unodc, https://www.unodc.org/roca/en/NEWS/2025/strengthening-uzbekistans-capacity-for-cross-border-justice_-digitalization-project-delivers-new-it-equipment-to-the-pgo.html

23. Battling Cybercrime Through the New Additional Protocol to the Budapest Convention, https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/

24. UN Convention Against Cybercrime Is a Huge Win! We've been trying to get something like this for decades. : r/cybersecurity - Reddit, https://www.reddit.com/r/cybersecurity/comments/1of1oqi/un_convention_against_cybercrime_is_a_huge_win/