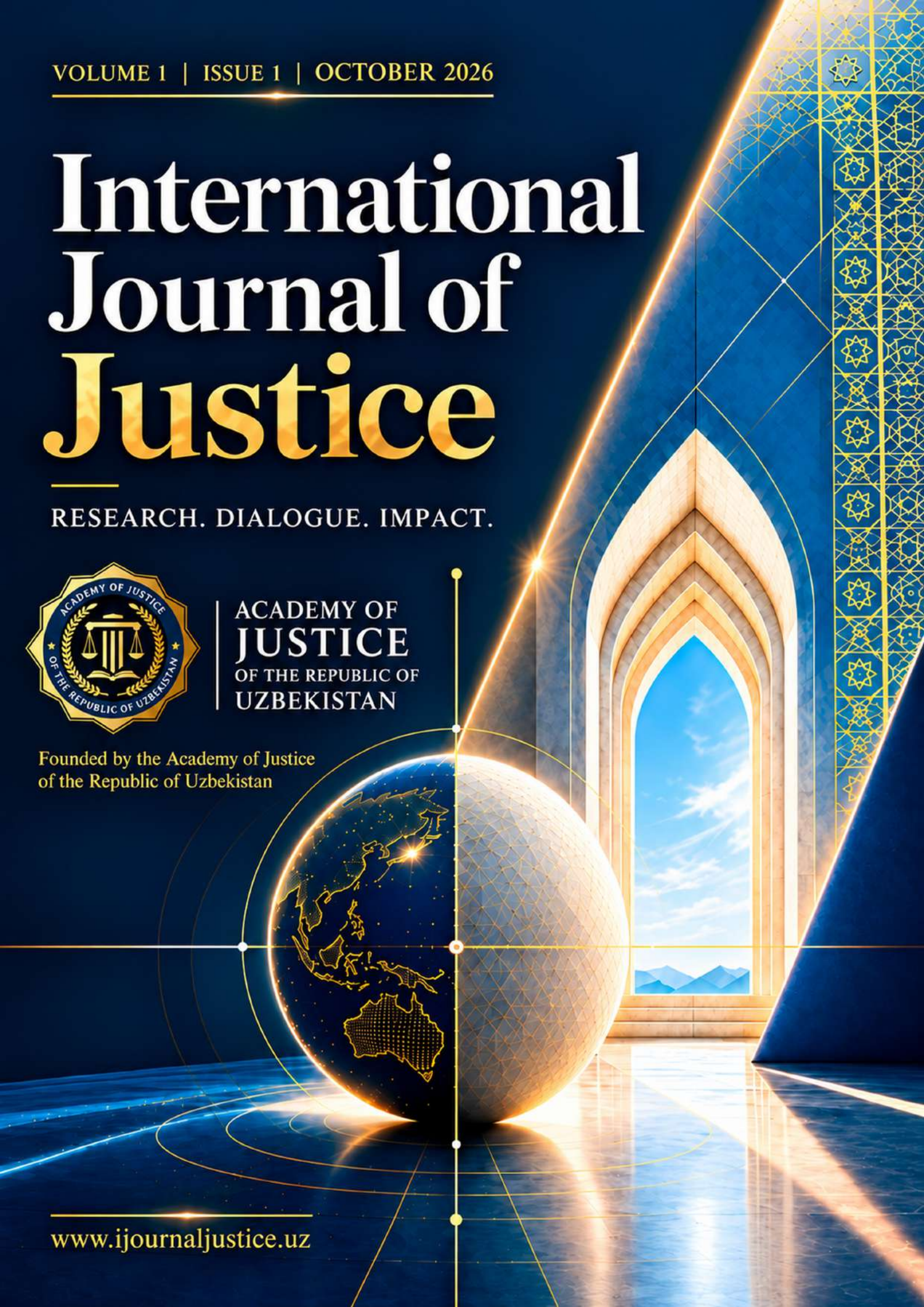
VOLUME 1 | ISSUE 1 | OCTOBER 2026

International Journal of Justice

RESEARCH. DIALOGUE. IMPACT.

ACADEMY OF JUSTICE OF THE REPUBLIC OF UZBEKISTAN

Founded by the Academy of Justice of the Republic of Uzbekistan



www.ijournaljustice.uz

EDITORIAL BOARD

International Journal of Justice



EDITOR-IN-CHIEF

Sherzod Yoqubjonovich Abduqodirov

Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Associate Professor



DEPUTY EDITOR-IN-CHIEF

Nodirbek Saparbaevich Salaev

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Professor

MEMBERS OF THE EDITORIAL BOARD



Anselmo Reyes

Doctor of Philosophy (PhD) in Law, Professor

Judge of the Singapore International Commercial Court



Dilshod Urinbaevich Aripov

Doctor of Sciences in Law (DSc), Professor

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan



Akrom Ikromovich Toshpulatov

Doctor of Sciences in Law (DSc), Professor

Director of the Parliamentary Research Institute under the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan



Shakhriyor Bakhtiyorovich Bakaev

Doctor of Philosophy (PhD) in Law

Responsible Official of the Administration of the President of the Republic of Uzbekistan



Borzu Sabahi

Doctor of Sciences in Law (DSc), Professor

International Arbitrator



Dilshod Shavkatovich Israilov

Doctor of Philosophy (PhD), Associate Professor

Head Specialist of the Department for Coordination of Research Activities of the Academy of Justice of the Republic of Uzbekistan



Yesemurat Sultamuratovich Kanyazov

Candidate of Legal Sciences in Law (PhD)

Director of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan



Yevgeniy Vyacheslavovich Kolenko

Doctor of Philosophy (PhD), Professor

First Deputy Head of the Law Enforcement Academy of the Republic of Uzbekistan



Krisztina Karsai
Doctor of Sciences in Law (DSc), Professor
Head of the Institute of Criminal Law and Criminal Sciences at the University of Szeged



Lorenzo Mateo Bujosa Vadell
Doctor of Philosophy (PhD) in Law, Professor
Professor at the University of Salamanca



Maged Mamdouh Kamel Shebaita
Doctor of Philosophy (PhD), Professor
International Arbitrator, Doctoral Candidate at the University of London



Ivan Georgievich Nikonov
Doctor of Philosophy (PhD) in Law
Responsible Official of the Administration of the President of the Republic of Uzbekistan



Malikakhon Pirnazarovna Kalandarova
Doctor of Philosophy (PhD), Associate Professor
Deputy Chairperson of the Supreme Court of the Republic of Uzbekistan



Islambek Rustambekovich Rustambekov
Doctor of Sciences in Law (DSc), Professor
Vice-Rector of Tashkent State University of Law



Sakari Kristian Melander
Doctor of Sciences in Law (DSc), Professor
Professor at the University of Helsinki



Khurshid Primkulovich Sadikov
Judge of the Supreme Judicial Council of the Republic of Uzbekistan



Sławomir Marek Redo
Doctor of Sciences in Law (DSc), Professor
Chairperson of the Expert Council for the Development of Scientific Research at the Faculty of Law and Administration



Vigita Vėbraitė
Doctor of Philosophy (PhD) in Law, Professor
Professor at Vilnius University



MANAGING EDITOR
Azamjon Rasuljon ugli Kambaraliev
Head Specialist at the Academy of Justice of the Republic of Uzbekistan

CONTENTS

IMPROVING THE INSTITUTION OF APPEALS: TIME LIMITS, RESPONSE QUALITY, MONITORING **10**
Achilova Liliya Ilkhomovna; Rozmetova Asal Anvarzoda

LEGAL ASPECTS OF INVESTIGATIVE JOURNALISM **18**
Jahonov Shohruh Shuhrat ugli

LEGAL BASIS OF CIVIL SOCIETY INSTITUTIONS IN THE LEGISLATION OF THE REPUBLIC OF UZBEKISTAN **25**
Sharipov Asrorjon Safar ugli

DIGITAL TRANSFORMATION OF INTERNATIONAL COMMERCIAL ARBITRATION IN UZBEKISTAN: LEGAL AND INSTITUTIONAL PROSPECTS **30**
Otakhonov Foziljon Khaydarovich

THE LEGAL NATURE OF SUBSIDIARY LIABILITY IN INSOLVENCY PROCEEDINGS INVOLVING AGRICULTURAL BUSINESS ENTITIES **39**
Rakhmatjon Tojinorovich Berdiyarov

CIVIL LAW ASPECTS OF GOODS DELIVERY BY SELF-EMPLOYED COURIERS **49**
Ruzinazarov Shukhrat Nuralievich

NATIONAL AND INTERNATIONAL EXPERIENCE IN LEGAL PROTECTION OF A COMPANY NAME: IMPROVING THE LEGISLATION OF UZBEKISTAN **63**
Allayarova Maftuna Almardanovna

ORGANIZATIONAL AND LEGAL MECHANISMS FOR COMPENSATION OF CONSTRUCTION CONTRACT DAMAGES **69**
Donayev Abduqodir Haydarovich

JURISDICTION AND VENUE OF CIVIL CASES ARISING FROM INHERITANCE RELATIONS: A NATIONAL AND FOREIGN ANALYSIS **76**
Soliyeva Kamola Rustamjon-qizi

ISSUES OF USING COURT NOTICES IN ENSURING THE OPENNESS OF CIVIL PROCEEDINGS IN COURTS **84**
Sabirov Erkinjon Kuchkarbaevich

DIGITAL EVIDENCE IN SUPPLY-CONTRACT DISPUTES BEFORE ECONOMIC COURTS: AUTHENTICATION, INTEGRITY AND EVIDENTIARY RISK IN UZBEKISTAN **91**
Mahmudova Saida Rayimjonovna

CONTENTS

FROM HUMAN CAPITAL TO INSTITUTIONAL TRANSFORMATION: A NEW STAGE IN THE STRATEGIC DEVELOPMENT OF THE JUDICIAL PERSONNEL TRAINING SYSTEM 104
Aripov Dilshod Urinbaevich

THE ROLE OF INTERNATIONAL STANDARDS IN GOVERNING ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS: A COMPARATIVE AND CRITICAL ANALYSIS 109
Sadikov Khurshid Primkulovich

INDEPENDENCE — A SOLID FOUNDATION OF JUSTICE AND HUMAN DIGNITY (35 years of the evolution of the judicial and legal system of the Republic of Uzbekistan) 117
Israilov Dilshod Shavkatovich

INSTITUTIONAL MODELS OF JUDICIAL QUALIFICATION BOARDS: INTERNATIONAL STANDARDS AND FOREIGN EXPERIENCE 128
Jamolov Azizjon Nodir ugli

THE DEATH OF FREE WILL. WHO BEARS CULPABILITY WHEN ARTIFICIAL INTELLIGENCE INDUCES A PERSON TO COMMIT A CRIME? 140
Salaev Nodirbek Saparbaevich

ON EUROPEAN CRIMINAL-LAW INTEGRATION – FROM MUTUAL RECOGNITION TO LIMITED SUPRANATIONAL CRIMINAL POWER 148
Krisztina Karsai

CRIMINAL LIABILITY OF OFFICIALS OF NON-GOVERNMENTAL COMMERCIAL ORGANIZATIONS: PROBLEMS OF THEORY AND PRACTICE 158
Akramova Muazzam Turdikul qizi

DISTINGUISHING OFFENCES AGAINST SEXUAL FREEDOM FROM RELATED OFFENCES IN UZBEKISTAN 162
Achilov Izzat Tulkinovich

CRIMINAL-LAW MEASURES AGAINST THE LEGALIZATION OF PROCEEDS OBTAINED THROUGH MISAPPROPRIATION OR EMBEZZLEMENT: QUALIFICATION, EVIDENCE AND ASSET RECOVERY 170
Sadullaev Bokhodir Oybekovich

CONCEPT OF HELPLESSNESS AND ITS SIGNIFICANCE IN THE QUALIFICATION OF CRIMES 178
Khalilova Zarnigor Zafar qizi

LEGAL SIGNIFICANCE OF THE INSTITUTION OF CRIMINAL RECORDS IN PROTECTING HUMAN RIGHTS 182
Yoqubjonov Omonjon Burkhonjon ugli

CONTENTS

THE APPLICATION OF CRIMES WITH BLANKET NORMS: CURRENT STATUS AND ISSUES 189
Pulatov Bekzod Adilbaevich

THE FORMATION AND DEVELOPMENT OF THE INSTITUTION OF CRIMINAL LIABILITY IN THE FIELD OF PUBLIC PROCUREMENT: A HISTORICAL-LEGAL ANALYSIS 202
Shukurova Shahnoza Mukumjonovna

ATTORNEY'S PARTICIPATION IN THE PRE-TRIAL STAGE OF CRIMINAL PROCEEDINGS: LEGAL AND PRACTICAL ASPECTS 214
Medetbaeva Aksungul Sharapatdin kizi

INTERNATIONAL COOPERATION IN OBTAINING ELECTRONIC EVIDENCE: THE EUROPEAN PRODUCTION AND PRESERVATION ORDERS 221
Bujosa Vadell, Lorenzo Mateo

COOPERATION BETWEEN THE SUBJECTS OF INVESTIGATION IN CROSS-BORDER INTERNET FRAUD CASES 230
Khabibiddinov Nodirjon Musinjon ugli

PROBLEMS OF PROCEDURAL REALITY IN CRIMINAL PROCEEDINGS 238
Aykhan Khankishi Rustamzade, Matanat Pasha Asgarova

DETENTION OF FOREIGN NATIONAL PRISONERS IN PENITENTIARY INSTITUTIONS: A COMPARATIVE ANALYSIS OF INTERNATIONAL PRACTICES AND NATIONAL LEGISLATION 246
Rikhsimov Komron Abrorovich

CRIMINALISTIC FOUNDATIONS FOR INTEGRATING GAIT IDENTIFICATION WITH FORENSIC PORTRAIT EXAMINATION 249
Nizomova Shahrigul Karimboy qizi

INTERNATIONAL LAW CRISIS: UN PEACE OPERATIONS AND INSTITUTIONAL REFORM 258
Kudaybergenov Bakhtiyar Abdumajit-ugli

ARTIFICIAL INTELLIGENCE AND CHILDREN'S RIGHTS: PROTECTION OPPORTUNITIES AND EMERGING LEGAL RISKS 267
Ergashev Gayrat Shavkatovich

ACTIVITIES OF INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS IN THE FIELD OF HUMAN RIGHTS 276
Nosirova Marjona Negmat kizi

Academy of Justice of the Republic of Uzbekistan
International Journal of Justice

DIGITAL EVIDENCE IN SUPPLY-CONTRACT DISPUTES BEFORE ECONOMIC COURTS: AUTHENTICATION, INTEGRITY AND EVIDENTIARY RISK IN UZBEKISTAN

Mahmudova Saida Rayimjonovna
Lecturer, Department of Economic and Legal Sciences,
Academy of Justice of the Republic of Uzbekistan
E-mail: s.mahmudova@sudacademy.uz
ORCID ID: 0009-0009-7884-0476



Abstract. *This article examines the legal treatment of digital evidence in disputes arising from supply contracts before the economic courts of the Republic of Uzbekistan. The research focuses on the procedural consequences of Law No. LRU-1003 of 21 November 2024, which introduced Articles 76¹ and 76² into the Economic Procedural Code and expressly regulated electronic data, digital evidence, copying, integrity, identity and the relationship between a digital source and its paper representation. The central problem is no longer whether electronically generated information can be evidence, but how courts should distinguish admissibility, authentication, integrity and probative weight when commercial facts are recorded in enterprise-resource-planning systems, electronic invoices, warehouse logs, transport-tracking data, electronic signatures, platform messages and screenshots. Using doctrinal, systemic, comparative-legal and scenario-based methods, the article analyses the Economic Procedural Code, legislation on electronic commerce, electronic document management, electronic digital signatures and personal data, together with UNCITRAL instruments, transnational procedural models and selected digital-evidence scholarship. It argues that Uzbekistan should avoid both paper-form formalism and technological deference. A digital record should not be rejected merely because it is not a traditional document, but neither should a system-generated record be treated as self-authenticating merely because it comes from business software. The article proposes a five-factor digital-evidence reliability matrix based on source attribution, integrity, temporal consistency, transactional linkage and adversarial verifiability; a controlled allocation of evidentiary risk under Articles 68 and 69; and a pretrial digital-evidence protocol for complex supply disputes. These measures are intended to improve predictability, procedural equality and the quality of judicial reasoning in technology-intensive commercial litigation.*

Keywords: *digital evidence; electronic data; economic court; supply contract; authentication; integrity; burden of proof; electronic commerce; evidentiary risk.*

Introduction

Commercial performance is increasingly recorded before it is ever described in a pleading. A supplier releases a batch through an enterprise-resource-planning system; a warehouse scan records loading; an electronic invoice identifies quantity and price; a transport platform records a route and timestamp; a buyer approves or rejects delivery through a procurement portal; and subsequent discussions take place through e-mail or messaging applications. When a dispute reaches an economic court, these records may be more probative than a later paper act prepared for litigation. The procedural question is therefore not whether technology has entered commercial evidence, but how law should determine which digital records are sufficiently connected to a disputed fact, sufficiently authentic, sufficiently intact and sufficiently open to adversarial verification to justify reliance. [1]

Uzbekistan moved from implicit recognition of electronic information to an express procedural architecture through Law No. LRU-1003 of 21 November 2024. The Law amended several procedural codes and, for economic proceedings, introduced Articles 76¹ and 76² into the Economic Procedural Code. Article 76¹ defines electronic data by reference to creation, processing and storage through electronic devices, information systems and information technologies. Article 76² defines digital evidence as electronic data containing information about circumstances relevant to the case and expressly includes electronic files, audio and video recordings, Internet information and other electronic data. The same provision requires integrity and identity to be preserved when digital evidence is copied and regulates the admissibility of copies and paper printouts. [2]

These rules are particularly important for supply-contract litigation because the substantive relationship itself generates dense streams of structured and semi-structured data. Articles 437-456 of the Civil Code regulate supply, while legislation on the contractual and legal framework of business entities and specialised Plenum guidance address recurring disputes concerning contractual performance, defective goods and failure to take delivery. The material facts usually concern formation and content of the contract, delivery time, quantity, assortment, quality, completeness, acceptance, inspection, notification, payment, damages and excuses for non-performance. Increasingly, each of these facts may be reflected in a different information system controlled by a different participant in the transaction. [3]

The resulting doctrinal problem has four dimensions. First, classification: when should an electronic record be treated as a digital evidence object rather than as a paper document merely because a printout exists? Second, authentication: what foundation sufficiently connects the record to the person, device, account or business system alleged to have generated it? Third, integrity: what is required to show that the information has not been materially altered between creation, extraction, submission and examination? Fourth, evidentiary risk: which party should bear the consequence of uncertainty when the decisive data are under the exclusive or predominant control of the opposing party or a third-party platform? Digital-evidence literature consistently shows that these dimensions should be separated rather than collapsed into a single question of whether a computer record is "reliable." [4]

The purpose of this article is to develop a supply-dispute-specific model for applying the new provisions. Its central hypothesis is that the best interpretation of the Economic Procedural Code is a staged model: relevance and statutory admissibility determine whether the digital material may enter the evidentiary record; a prima facie authentication foundation connects the material to its alleged source; integrity and identity are tested through technical and contextual indicators; and final probative weight is assessed under Article 74 together with the complete evidentiary record. The article further argues that information asymmetry should be addressed through targeted production, adverse consequences for unjustified withholding and pretrial evidence management rather than an unstructured reversal of the ultimate burden of proof.

2. Materials and Methods

The research is doctrinal and applied. The primary national sources are the Economic

Procedural Code, including Articles 66-76² and 163¹; Law No. LRU-1003 of 21 November 2024; the Civil Code provisions governing supply; Law No. 670-I on the contractual and legal framework of business entities; Law No. LRU-792 on electronic commerce; Law No. LRU-793 on electronic digital signatures; Law No. 611-II on electronic document management; Law No. LRU-547 on personal data; and relevant Plenum resolutions concerning contractual disputes. The legislation was examined in the version in force on 7 September 2026. [5]

Four methods were applied. The formal-doctrinal method was used to identify the statutory elements of electronic data, digital evidence, copies, originals, written evidence, burden of proof and judicial evaluation. The systemic method examined the interaction between procedural evidence rules and the legal rules governing electronic contracting, electronic signatures, storage of commercial records and protection of personal data. The comparative method used UNCITRAL instruments, the ALI/UNIDROIT Principles of Transnational Civil Procedure, the ELI/UNIDROIT Model European Rules of Civil Procedure, selected United States authentication rules and technical preservation standards as functional comparators rather than as sources of directly applicable law. The scenario method tested the proposed model against recurrent supply-dispute fact patterns involving electronic invoices, ERP records, GPS data, warehouse logs, messaging-platform correspondence and screenshots. [6]

The comparative approach is deliberately limited. Digital evidence cannot be detached from domestic rules on admissibility and judicial proof. A technical hash, a server log or an electronic signature may be highly informative, but no technical indicator by itself determines the legal effect of a record. Conversely, legal categories such as "original" and "copy" may become difficult to apply to cloud-native or database-generated information if they are interpreted as if every electronic record existed as one unique physical object. The analysis therefore uses functional equivalence: the legal purpose behind a requirement is identified first, and only then is the technological mechanism assessed as a possible way of satisfying that purpose. [7]

Results

3.1. The procedural architecture after Law No. LRU-1003

The 2024 reform establishes an important distinction between electronic data and digital evidence. Electronic data are defined broadly by the technological manner in which they are created, processed and stored. Digital evidence is narrower in functional terms: it is electronic data containing information about circumstances relevant to the case. Thus, an entire server, device or database may contain electronic data, while only a defined subset may have evidentiary relevance to a particular dispute. This distinction is useful because it prevents the concept of digital evidence from becoming coextensive with every piece of information stored on a device. [8]

Article 76¹ also regulates the act of presentation. Parties, witnesses and other participants may present electronic data by copying them from one electronic carrier to another, while the court, with the participation of a specialist, accepts the data and examines the primary electronic carrier. Article 76² then permits copying of digital evidence only if integrity and identity are preserved. These provisions reveal two separate concerns: procedural access to the data and evidentiary

confidence that the submitted representation corresponds to the relevant source. They should not be treated as synonyms. A party may technically succeed in copying a file, yet still fail to explain who created it, whether it belongs to the relevant transaction or whether it was altered after creation.

The Code further provides that admissibility of a copy is ensured by the existence of the original from which the copy was made, except for notarised digital evidence. Parties and other participants may submit digital evidence printed on paper, but the paper representation is not itself written evidence, again subject to the notarisation exception. The distinction is doctrinally significant. It rejects a common evidentiary shortcut: transforming a digital source into a paper document merely by printing a screenshot, e-mail, spreadsheet or platform page. The legal object remains digital, and the paper serves at most as a representation through which its visible content may be reviewed. [9]

This approach is consistent with the broader national framework for electronic commerce. Law No. LRU-792 recognises electronic documents and identifiable electronic messages as capable of evidencing contract formation, recognises specified electronic confirmation methods, and permits commercial processes and performance documents to operate electronically. Law No. LRU-793 gives legal significance to electronic digital signatures, while Law No. 611-II supplies the general framework for electronic document management. These statutes establish substantive legal force; the Economic Procedural Code determines how the resulting information is proved in litigation. The two layers must be read together. [10]

3.2. Admissibility, authentication, integrity and probative weight

A coherent digital-evidence doctrine requires four questions to be asked in sequence. Admissibility asks whether the evidence is of a legally permissible form and whether any statutory condition for its use has been satisfied. Authentication asks whether there is a sufficient foundation to conclude that the record is what its proponent claims it to be. Integrity asks whether the informational content and relevant metadata have remained materially unchanged through creation, storage, extraction and submission. Probative weight asks how strongly the authenticated and admissible record supports the fact for which it is offered. Article 74 supports this separation by requiring individual evidence to be evaluated for relevance, admissibility and reliability and the totality of evidence for sufficiency, while denying predetermined force to any item. [11]

Authentication should therefore be understood as a threshold foundation, not as final proof of truth. An electronic invoice may be authenticated as a record generated by the supplier's invoicing system without proving that the quantity stated in it was actually delivered. A GPS log may be authenticated as data exported from a carrier's tracking system without proving that the tracked vehicle carried the disputed goods. A messaging account may be linked to an employee without proving that every statement made through the account was accurate or authorised. Comparative evidence law similarly treats authentication as a showing that supports identification of the item, leaving persuasive weight for later evaluation. [12]

Integrity is related but distinct. The statutory terms "integrity" and "identity" in

Article 76² should be operationalised through a combination of technical and contextual evidence. Potential technical indicators include hash values for exported files, audit logs, electronic-signature verification, system-generated identifiers, metadata, access-control records, immutable transaction logs and documented extraction procedures. Contextual indicators include consistency with accounting records, bank payments, warehouse movements, subsequent correspondence, physical inspection and the behaviour of the parties. Neither type should be mechanically privileged. A technically perfect copy of a fabricated source remains fabricated; a record lacking a forensic hash may still be reliable if its source, chronology and business context are independently corroborated. [13]

This distinction also clarifies the role of a specialist. Article 76¹ requires specialist participation when the court accepts presented electronic data and examines the primary electronic carrier. Specialist assistance may be essential for accessing a database, verifying an export, explaining metadata or preserving a source. It should not, however, displace the judicial function under Article 74. The specialist can explain the system and technical integrity; the court must still determine relevance, admissibility, reliability and sufficiency in light of the parties' arguments and the whole case.

3.3. The problem of the "original" in distributed and cloud systems

Article 76² conditions admissibility of a copy on the existence of the original from which it was produced. For ordinary files stored on a local device this formulation is relatively straightforward. Commercial systems, however, increasingly store data in replicated databases, cloud environments, enterprise systems and platform infrastructures where there may be no single physical "original" analogous to the signed sheet of paper. The authoritative record may be a database state reconstructed from entries, a server-side event log, an export generated on demand or a record distributed across several storage layers. Digital-evidence scholarship has long cautioned against importing paper-based originality concepts without considering how computer systems create and reproduce information. [14]

The Code should not be read as eliminating the original requirement, but its purpose should be specified. The purpose is to ensure that the copy submitted to the court can be verified against an authoritative source and that the process of reproduction has not changed the evidentiary content. In a cloud-native system, the "original" should therefore be identified by reference to the authoritative source environment, dataset or controlled system state from which the representation was extracted. This is an interpretative proposal, not a claim that the statutory wording already expressly defines cloud originals in this way.

A party relying on a cloud or platform record should accordingly identify the system, account or tenant, relevant record identifier, extraction method, date and time of export, and any verification data available. Where the source is controlled by a third-party platform, the party should explain the obtainable verification route, such as an official export, provider confirmation, electronically signed record, API record or other system-level indicator. Courts should resist the opposite extremes of demanding physical seizure of infrastructure that cannot realistically be brought to court and accepting an unexplained

screenshot as the functional equivalent of the primary source.

3.4. Evidence generated by commercial information systems

ERP, warehouse-management and logistics systems present a recurring evidentiary pattern: the record may be generated automatically in response to a human action, generated entirely by the system, or generated through a combination of automated and manual inputs. These categories matter because they create different authentication questions. A user-entered delivery confirmation requires proof connecting the account to an authorised user and the entry to the transaction. A sensor-generated timestamp requires confidence in the device or system process. A calculated inventory balance may require explanation of the input data and software logic. Machine-generated evidence literature illustrates why attribution to a human declarant is not always the correct analytical model. [15]

For supply disputes, the relevant foundation should normally answer six questions: what system generated the record; what event caused its creation; who or what had authority to create or alter it; whether the timestamp and identifier correspond with other transaction records; whether logs or metadata reveal later modification; and whether the record can be linked to the specific contract, invoice, batch, consignment or delivery. The purpose is not to require expert evidence for every electronic invoice. Routine records may be authenticated through ordinary business evidence. Technical assistance becomes proportionate when authenticity is genuinely disputed, the system is complex or the record is decisive.

Electronic signatures are a particularly strong but not absolute indicator. Under the national electronic-signature regime, a valid electronic digital signature performs identification and integrity functions. In a supply dispute, successful signature verification may establish a powerful connection between a document and a signature key. It does not necessarily prove authority beyond the scope of the key, correctness of the underlying commercial statement, absence of duress or fraud, or actual performance of the obligation. Signature evidence should therefore be treated as part of authentication and integrity analysis, not as predetermined proof of the substantive fact asserted. [16]

3.5. Screenshots, messaging applications and platform correspondence

Screenshots are convenient because they preserve visible content, but their convenience also creates evidentiary weakness. A screenshot may omit the account identifier, metadata, complete conversation context, deleted messages, editing history, time-zone information or the technical source from which the image was captured. It may also be cropped or altered without obvious visual signs. A categorical rule excluding screenshots would nevertheless be excessive. Screenshots may provide useful corroboration, especially when the opposing party admits the communication or when content is confirmed by surrounding evidence. Comparative writing on social-media authentication similarly supports a contextual rather than categorical approach. [17]

Where a screenshot is materially disputed, the court should seek the best reasonably available verification source: device inspection, a platform export, account data, surrounding

messages, electronic-signature information, provider records where lawfully obtainable, or specialist examination. The proponent should not be required to achieve technical perfection that the platform itself makes impossible, but should explain why the submitted representation is a faithful record of the communication. Conversely, a bare allegation of manipulation should not automatically neutralise evidence where the record is strongly corroborated.

The same analysis applies to messages used to prove modification of delivery terms, acceptance, notification of defects or acknowledgement of debt. The legal significance of the communication must be separated from its evidentiary authenticity. First the court determines whether the message is attributable and intact; then it determines whether the content, under substantive contract law and the parties' agreement, was capable of producing the asserted legal consequence.

3.6. Allocation of evidentiary risk and information control

Article 68 retains the general rule that each participant must prove the circumstances relied on as the basis of claims and objections. It also requires disclosure before the hearing or within the time fixed by the court and creates an adverse consequence where a party withholds evidence requested by the court: the information contained in the evidence is presumed adverse to that party and treated as admitted. Article 69 enables participants unable to obtain necessary evidence independently to seek judicial assistance in obtaining it. These provisions are well suited to digital information asymmetry. [18]

The ultimate legal burden should not shift merely because relevant information is digital. A supplier claiming the contract price still bears the burden of establishing the constitutive facts of its claim. A buyer relying on payment, timely rejection or another independent defence bears the burden attached to that defence. What may shift dynamically is the evidential burden to respond to a prima facie showing or the production burden when one party controls the best record. Procedural scholarship distinguishes these burdens because collapsing them can either unfairly penalise the information-poor party or destabilise substantive allocation of proof. [19]

A controlled model has three stages. First, the party bearing the ultimate burden identifies the disputed fact and presents a prima facie evidentiary basis. Second, if a material digital source is predominantly controlled by the opponent or a third person, the party identifies the source with enough specificity for Article 69 production. Third, if the controller fails without justification to produce evidence ordered by the court, Article 68 supplies the procedural consequence. This model is preferable to an abstract statement that "the burden shifts" because it identifies what burden shifts, why it shifts and what legal consequence follows.

3.7. A five-factor digital-evidence reliability matrix

The following five-factor matrix is proposed for digital evidence in supply disputes. First, source attribution: can the record be linked to the relevant person, account, device, information system or business process? Second, integrity: is there a reasonable basis for concluding that relevant content has not been materially altered between creation and examination? Third, temporal consistency: do timestamps,

sequence numbers and surrounding events fit the transaction chronology? Fourth, transactional linkage: can the record be connected to the particular contract, invoice, batch, consignment, payment or notice in dispute? Fifth, adversarial verifiability: has the opposing party received a meaningful opportunity to inspect the source, a reliable copy or sufficient technical information to challenge authenticity and weight? [20]

The matrix is not a statutory list of cumulative admissibility conditions. It is a judicial reasoning tool. Different factors may carry different weight depending on the evidence. An electronically signed invoice may have strong attribution and integrity but weak proof of physical delivery. A warehouse video may have strong transactional linkage but require more work on timestamp integrity. A platform export may be highly verifiable but depend on a third-party provider. The matrix makes the reasons for reliance visible and therefore improves appellate review and party predictability.

Discussion

4.1. Functional equivalence and the limits of paper-form thinking

UNCITRAL's Model Law on Electronic Commerce supplies a useful conceptual comparison because it rejects discrimination against information merely because it is in the form of a data message and directs attention to reliability, integrity and the manner in which information was generated, stored or communicated when evidential weight is assessed. Uzbekistan's current procedural rules are not identical to the Model Law, but the functional insight is compatible with the national reform: the decisive inquiry is whether the electronic form performs the legal and evidentiary function required, not whether it resembles paper. [21]

The national Law on Electronic Commerce reinforces this approach by giving legal significance to electronic documents and identifiable electronic messages and by regulating electronic formation, acceptance and storage. These substantive rules would be weakened if economic courts required parties to convert every relevant record into a conventional paper document before treating it seriously. Article 76² appropriately prevents that conversion from changing the evidentiary category. The paper printout is a representation of a digital source, not a magical transformation of that source into written evidence.

Functional equivalence must, however, remain disciplined. It cannot mean that every electronic output is presumptively authentic. The principle removes discrimination based on form; it does not remove authentication. A forged electronic document, fabricated screenshot or manipulated database export is not made reliable by the fact that electronic commerce is legally recognised. The evidentiary regime must remain capable of testing source, integrity and context.

4.2. Comparative procedural standards and technical preservation

The ELI/UNIDROIT Model European Rules of Civil Procedure define documents broadly enough to include electronic forms and distinguish the burden of proof from the burden to adduce evidence. The ALI/UNIDROIT Principles likewise emphasise fair opportunity to present and respond to evidence in transnational commercial adjudication. These materials support two propositions relevant to Uzbekistan: electronic evidence should be treated as an ordinary

evidentiary category rather than an exceptional technological object, and procedural equality requires meaningful access to the information needed to test the opponent's digital case. [22]

Technical standards such as ISO/IEC 27037 and NIST SP 800-86 are useful for preservation, acquisition and documentation. They can help experts and specialists explain good practice in identifying, collecting, acquiring and preserving digital information. They should not be converted into rigid legal admissibility rules unless national legislation expressly does so. A commercial litigant should not lose a meritorious claim merely because a routine business record was not collected according to a forensic-investigation standard developed for different contexts. Technical standards are most persuasive where authenticity is contested, evidence is volatile or forensic acquisition has actually been undertaken. [23]

Comparative United States practice also illustrates the distinction between authentication and final weight. Federal Rule of Evidence 901 requires a foundation sufficient to support a finding that the item is what the proponent claims; Rules 902(13) and 902(14) create mechanisms for certain certified electronic records and data copied from devices; and the original-writing rules recognise that digital information challenges traditional notions of originality. Lorraine v. Markel remains influential because it demonstrates that electronic evidence must be analysed through ordinary evidentiary requirements rather than admitted merely because it appears technologically familiar. The comparison is instructive, but the governing law in Uzbek economic courts remains the Economic Procedural Code. [24]

4.3. Risks of excessive formalism and excessive technological deference

The first risk is excessive formalism. A court may insist on a traditional paper act despite the existence of a more complete and reliable digital record, or treat a screenshot as unusable solely because source metadata were not initially filed. This approach raises litigation costs and may reward the party that controls the underlying system. The second risk is excessive technological deference: assuming that an ERP entry, electronic signature, platform export or automated timestamp is correct because it was generated by software. Modern scholarship on machine evidence cautions that systems are designed, configured and fed by humans and may contain errors, biased inputs or incomplete logs. [25]

The balanced approach is proportional authentication. The depth of the foundation should correspond to the importance of the evidence and the seriousness of the challenge. Routine electronic invoices admitted by both parties require little technical proof. A decisive disputed ERP export created after litigation began may require metadata, audit logs and specialist explanation. A messaging screenshot corroborated by payment and delivery records may be sufficient without platform-level production. A screenshot standing alone, denied by the alleged sender and lacking account information, requires a stronger foundation.

4.4. Pretrial digital-evidence management

Article 163[1] provides a procedural stage at which the judge may clarify claims, objections and the evidence supporting them. Complex digital-evidence disputes should use this stage to create a concise digital-evidence protocol. The protocol should identify the disputed

digital sources, the party or third person controlling each source, the required form of production, any integrity or authentication issue already raised, whether specialist assistance is needed, and deadlines for inspection or objections. This would not transform the judge into an investigator; it would make the parties' evidentiary responsibilities explicit before the merits hearing. [26]

A protocol is especially valuable where evidence is volatile. Messaging histories may be deleted, cloud logs may be retained only for limited periods, platform accounts may change, and business systems may overwrite audit information. Early identification also permits proportionate preservation: the court need not order production of an entire server when a defined export, log segment or transaction history will resolve the issue. Personal-data protection must be integrated by limiting production to relevant information and using procedural safeguards for unrelated personal data. [27]

4.5. Practical application to recurring supply scenarios

Consider five simplified situations. In the first, the supplier presents an electronically signed invoice and an ERP dispatch record; the buyer admits receipt but denies quantity. Authentication is largely established, but the decisive issue is transactional linkage to quantity, requiring warehouse or acceptance evidence. In the second, the buyer presents a screenshot of a messenger conversation allegedly extending the delivery deadline; the supplier denies authorship. The court should seek account attribution, surrounding messages or a device/platform source rather than treating the screenshot as conclusive or worthless. In the third, a carrier's GPS export is offered to prove arrival at the buyer's warehouse. The record must be linked to the relevant vehicle and consignment, and its timestamp tested against other delivery records.

In the fourth situation, a buyer claims that defective goods were timely reported through an electronic procurement portal controlled by the supplier. The buyer produces a confirmation e-mail but lacks the underlying portal log. If the e-mail and surrounding evidence create a prima facie basis, targeted production under Article 69 should be used; unjustified withholding by the controller may trigger Article 68 consequences. In the fifth, a party produces only a paper printout of an online account statement. Article 76^2 prevents the court from silently reclassifying the printout as written evidence; the party must identify and, where necessary, make available the digital source or a qualifying notarised digital record.

4.6. Legislative and interpretative improvements

First, Supreme Court guidance should expressly distinguish admissibility, authentication, integrity and probative weight for digital evidence. Second, guidance should explain the operation of "original" and "primary electronic carrier" for cloud, platform and database systems, focusing on access to an authoritative source and verifiable reproduction without contradicting Article 76^2. Third, courts should use a proportional authentication approach and avoid imposing forensic-level requirements on uncontested routine commercial records.

Fourth, Article 163^1 practice should incorporate a digital-evidence protocol in complex cases. Fifth, standard judicial reasoning should identify the digital source,

the authentication foundation, integrity indicators, the material fact supported, competing evidence and the reason for the assigned weight. Sixth, procedural training should include ERP logs, electronic invoices, digital signatures, screenshots, messaging exports, GPS records and cloud evidence. Seventh, preservation and production orders should incorporate data minimisation where personal data or unrelated business information are present.

Finally, the relationship between the rules on digital evidence and existing Plenum guidance for supply disputes should be modernised. Resolutions drafted around paper acts remain valuable for defining legally material facts, but evidentiary checklists should expressly recognise equivalent digital records where the Code's requirements are satisfied. The goal is not to abolish documentary discipline; it is to ensure that the form in which a fact is recorded does not obscure the substantive and procedural function of the evidence.

Conclusion and Practical Proposals

The introduction of Articles 76^1 and 76^2 marks a structural change in Uzbek economic procedure. Digital information is no longer accommodated only through general documentary concepts; the Code now defines electronic data and digital evidence, regulates copying, requires integrity and identity, distinguishes a paper printout from written evidence and preserves a connection between a copy and its original source. For supply-contract disputes, this reform is especially significant because modern performance is recorded across multiple commercial information systems.

The study confirms that the principal challenge has shifted from recognition to evaluation. Courts need to distinguish four questions: legal admissibility, source authentication, integrity of the informational object and final probative weight. Authentication is a threshold foundation, not proof of truth. Integrity should be established through converging technical and contextual indicators rather than through one mandatory technology. Electronic signatures are powerful evidence of attribution and integrity but do not automatically prove substantive performance. Screenshots can corroborate a case but require stronger verification when authorship or completeness is materially disputed.

The following practical proposals are advanced: (1) adopt Supreme Court guidance separating admissibility, authentication, integrity and weight; (2) operationalise the concepts of "original" and "primary electronic carrier" for cloud and database evidence; (3) apply a five-factor reliability matrix covering source attribution, integrity, temporal consistency, transactional linkage and adversarial verifiability; (4) preserve the ultimate burden of proof under Article 68 while using Article 69 production and Article 68 adverse consequences to address digital information asymmetry; (5) introduce a pretrial digital-evidence protocol under Article 163^1 for complex disputes; (6) modernise supply-dispute Plenum guidance to recognise reliable digital equivalents of traditional documents; (7) require element-by-element reasoning when courts rely on contested digital evidence; and (8) integrate personal-data minimisation and proportional preservation into production orders.

These proposals do not create a technologically exceptional law of proof. Their purpose is to make ordinary procedural principles work accurately in a digital

commercial environment. A court should neither distrust a record because it is electronic nor trust it because it is generated by software. The correct question is whether the record can be connected to the disputed transaction, shown to be sufficiently intact and examined fairly by the opposing party within the evidentiary structure of the Economic Procedural Code.

References

1. Economic Procedural Code of the Republic of Uzbekistan, 24 January 2018, Arts. 66-76²; Law of the Republic of Uzbekistan No. LRU-1003 of 21 November 2024.

2. Law of the Republic of Uzbekistan No. LRU-1003 of 21 November 2024, Art. 7; Economic Procedural Code, Arts. 76¹ and 76².

3. Civil Code of the Republic of Uzbekistan (Part Two), Arts. 437-456; Law No. 670-I of 29 August 1998; Resolutions of the Plenum of the Higher Economic Court Nos. 174 and 175 of 28 December 2007, as amended.

4. Mason, S., and Seng, D. (eds.), Electronic Evidence, 4th ed. (London: Institute of Advanced Legal Studies, 2017); Casey, E., Digital Evidence and Computer Crime, 3rd ed. (Elsevier Academic Press, 2011); Paul, G.L., Foundations of Digital Evidence (Chicago: American Bar Association, 2008).24. Paul, G.L. Foundations of Digital Evidence. Chicago: American Bar Association, 2008.

5. Economic Procedural Code of the Republic of Uzbekistan; Laws Nos. LRU-1003, LRU-792, LRU-793, 611-II, LRU-547 and 670-I, in force as of 7 September 2026.

6. UNCITRAL Model Law on Electronic Commerce (1996); UNCITRAL Model Law on Electronic Signatures (2001); ALI/UNIDROIT Principles of Transnational Civil Procedure (2004); ELI/UNIDROIT Model European Rules of Civil Procedure (2020); ISO/IEC 27037:2012; Federal Rules of Evidence, Rules 901 and 902.

7. UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment 1996, especially Arts. 8-10; Mason and Seng, Electronic Evidence; Biasiotti, M.A. et al. (eds.), Handling and Exchanging Electronic Evidence Across Europe (Cham: Springer, 2018).

8. Economic Procedural Code, Arts. 76¹ and 76².

9. Economic Procedural Code, Art. 76². The provision permits paper printouts but expressly states that the paper form is not written evidence, except for notarised digital evidence.

10. Law No. LRU-792 "On Electronic Commerce", Arts. 14-19; Law No. LRU-793 "On the Electronic Digital Signature"; Law No. 611-II "On Electronic Document Management".

11. Economic Procedural Code, Art. 74; Skontzos, A.V., "The Burden and Standard of Proof in Model International Procedural Law," Uniform Law Review 23, nos. 3-4 (2018): 569-592.

12. Federal Rules of Evidence, Rule 901; Grimm, P.W., Bergstrom, L.Y., and O'Toole-Loureiro, M.M., "Authentication of Social Media Evidence," American Journal of Trial Advocacy 36 (2013): 433-458; Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).

13. ISO/IEC 27037:2012; Kent, K. et al., Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86 (2006); Casey, Digital Evidence and Computer Crime.

14. Mason and Seng, Electronic Evidence; Paul, Foundations of Digital Evidence; Kerr, O.S., "Digital Evidence and the New Criminal Procedure," Columbia Law Review 105, no. 1 (2005): 279-318.

15. Roth, A.L., "Machine Testimony," Yale Law Journal 126, no. 7 (2017): 1972-2053; Casey, Digital Evidence and Computer Crime.

16. Law No. LRU-793 "On the Electronic Digital Signature"; UNCITRAL Model Law on Electronic Signatures (2001).

17. Grimm, Bergstrom and O'Toole-Loureiro, "Authentication of Social Media Evidence," 433-458; Lorraine v. Markel, 241 F.R.D. 534.

18. Economic Procedural Code, Arts. 68 and 69.

19. Sanchirico, C.W., "The Burden of Proof in Civil Litigation: A Simple Model of Mechanism Design," International Review of Law and Economics 17, no. 3 (1997): 431-447; Skontzos, "The Burden and Standard of Proof"; Brinkmann, M., "The Synthesis of Common and Civil Law Standard of Proof Formulae in the ALI/UNIDROIT Principles," Uniform Law Review 9, no. 4 (2004): 875-891.

20. Mason and Seng, Electronic Evidence; ISO/IEC 27037:2012; ELI/UNIDROIT Model European Rules of Civil Procedure, Rule 111.

21. UNCITRAL Model Law on Electronic Commerce (1996), Arts. 5, 8 and 9; United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

22. ELI/UNIDROIT Model European Rules of Civil Procedure (2020), including Rules 25 and 111; ALI/UNIDROIT Principles of Transnational Civil Procedure (2004); Stürner, R., "The ELI/UNIDROIT Model European Rules of Civil Procedure," RabelsZ 86 (2022): 421-450.

23. ISO/IEC 27037:2012; Kent et al., NIST Special Publication 800-86. These are technical and practitioner standards, not independent sources of admissibility under Uzbek procedural law.

24. Federal Rules of Evidence, Rules 901, 902(13), 902(14) and 1001-1003; Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).

25. Roth, "Machine Testimony," 1972-2053; Kerr, "Digital Evidence and the New Criminal Procedure," 279-318; Paul, Foundations of Digital Evidence.

26. Economic Procedural Code, Art. 163¹.

27. Law No. LRU-547 "On Personal Data"; Law No. LRU-792 "On Electronic Commerce", including provisions concerning storage and protection of electronic documents and messages.

