Evaluation of the Regulatory Framework for Digital Information in Criminal Proceedings

Toghrul Malikzada [1]

[1] *Forensic Expertise Centre, Ministry of Justice of the Republic of Azerbaijan*
24 Khagany, Baku, AZ1000, Azerbaijan

DOI: 10.22178/pos.131-3

JEL Classification: K39

Received 16.05.2025
Accepted 27.06.2026
Published online 30.06.2026

Corresponding Author:
Toghrul Malikzada

Abstract. The rapid digitalisation of criminal proceedings has increased the evidentiary importance of electronically stored information and has created new challenges for admissibility, reliability, data integrity, and the protection of fair-trial rights. This study evaluates the regulatory framework governing digital information in criminal proceedings, with particular attention to the collection, preservation, verification, and use of digital evidence in national and transnational investigations. The research applies comparative legal analysis, black-letter legal analysis, and content analysis of scholarly literature, international standards, and selected criminal justice practices from 2018 to 2025. The study examines procedural and technical requirements, including the legality of acquisition, documentation of all stages of handling, chain of custody, source identification, secure storage, audit mechanisms, and the use of verified forensic tools. The findings show that the legal validity of digital evidence depends on the coordinated interaction of procedural safeguards and technical standards. Jurisdictions with more developed regulatory systems demonstrate stronger mechanisms of automated logging, multi-level access control, certification, and regular verification. At the same time, states with less formalised procedures face higher risks of evidentiary challenges, loss of integrity, and violations of participants' rights. The study argues that national regulation should be harmonised with international standards, including ISO/IEC 27037:2012 and Council of Europe approaches to electronic evidence. It recommends adopting clear admissibility criteria, mandatory documentation rules, regular procedural audits, professional training, and methodological guidelines for investigators, forensic experts, prosecutors, defence lawyers, and judges. These measures can strengthen evidentiary reliability, procedural fairness, and cross-border cooperation in digital criminal justice.

Keywords: digital evidence; criminal proceedings; legal regulation; admissibility of materials; international standards; electronic information; procedural rules; chain of custody; digital forensics; evidence integrity; fair trial; cross-border data exchange; regulatory gaps.

INTRODUCTION

In recent years, digital technologies have become integral to criminal proceedings, raising critical questions about the admissibility, collection, and preservation of electronic evidence. The rapid development of information technologies has outpaced the legal frameworks of most countries, creating gaps in both national and international regulation [1]. Contemporary research emphasises the need to standardise procedures for evaluating digital materials and align their use with international standards and best practices, including the guidance of the Cybercrime Convention Committee and the Federal Rules of Evidence [2, 3].

Modern approaches to electronic evidence are increasingly conceptualised as a comprehensive system that integrates legal norms, technical methodologies, and principles for protecting the rights of participants in criminal proceedings [4–6]. The scientific novelty of this study lies in the development of criteria for evaluating digital evi-

dence that consider both national legislation and international practices, while also identifying potential risks to participants' rights in cross-border information exchange [7]. In addition, the study addresses challenges arising from transnational investigations and highlights the importance of procedural safeguards to maintain evidentiary reliability [8, 9].

This study aims to conduct a comprehensive assessment of the regulatory framework governing digital information in criminal proceedings. To achieve this aim, the following objectives have been formulated:

1) Analysis of the current legal framework;

2) Identification of problematic aspects concerning the admissibility and preservation of electronic materials;

3) Examination of foreign practices, including comparative insights from the UAE, USA, and European jurisdictions [10, 11]; and

4) Development of recommendations for improving regulatory standards. The relevance of this work is underscored by the increasing number of technology-related crimes and the need to enhance the efficiency, fairness, and reliability of the judicial system in handling digital evidence [12–17].

Research Problem. The increasing prevalence of crimes involving information technology and the growing volume of electronic materials used in courts highlight the critical importance of analysing the regulatory framework for digital information in criminal proceedings. In the contemporary legal landscape, it is essential to assess existing laws to identify gaps, inconsistencies, and ambiguities that may impede the fair adjudication of cases and compromise the protection of participants' rights.

The findings of this study are expected to contribute to enhancing judicial practice by developing clear criteria for the admissibility, reliability, and preservation of digital evidence. Additionally, the research aims to inform improvements in legal regulation at both national and international levels. For the scientific community, this work will provide a systematic analysis of existing approaches, identify legislative gaps, and propose recommendations to harmonise regulatory standards with international best practices.

Despite ongoing research on digital evidence across various jurisdictions, its legal regulation remains underdeveloped, particularly regarding cross-border information exchange, authenticity verification, and procedural control. This study seeks to identify emerging patterns and methodologies for evaluating digital sources and to propose practical solutions to improve legislation and ensure higher-quality judicial proceedings.

Research Focus. The primary focus of this research is to analyse the regulatory framework governing digital information in criminal proceedings and identify gaps, shortcomings, and contradictions in existing legislation. Particular attention is given to the criteria for admissibility and reliability of electronic evidence, as well as to the procedures for its collection, storage, and use in judicial practice, including a comparative analysis of national and international standards.

The study seeks to systematise existing approaches to digital evidence, evaluate their practical significance, and identify opportunities for legislative improvement. Emphasis is placed on developing effective legal regulatory methods that balance protecting the rights of participants in criminal proceedings with ensuring the efficiency and integrity of judicial processes in an increasingly digitalised environment.

Research Aim and Research Questions. The study aims to provide a theoretical, legal, and practical justification for the regulatory framework governing digital information in criminal proceedings, with particular emphasis on the admissibility, reliability, and integrity of electronic evidence in accordance with digital forensics standards and the principles of a fair trial. The research focuses on identifying gaps and inconsistencies within the current legal framework and developing practical recommendations to enhance the efficiency and quality of judicial practice.

The following research areas have been identified to achieve this objective:

a) Studying modern approaches to the legal understanding of digital evidence in criminal proceedings;

b) Identifying key procedural and technical conditions for the admissibility and reliability of electronic materials;

c) Analysing the importance of the chain of custody and procedural control for ensuring data integrity;

d) Assessing the consequences of violations in the collection, processing and presentation of

digital evidence for the realisation of the right to a fair trial;

e) Developing guidelines for the proper use of digital information in criminal proceedings.

In line with the issues identified, the study seeks to answer the following questions: how do procedural rules and standards of digital forensics interact in the assessment of digital evidence; what criteria determine their admissibility; how does a breach of the chain of custody affect the probative value of information; how is the balance between the effectiveness of criminal prosecution and the guarantees of a fair trial ensured?

Literature Review

An analysis of recent publications indicates that digital evidence is increasingly becoming a critical component of criminal proceedings, necessitating a clear regulatory framework to ensure its admissibility, reliability, and integrity. Current research primarily focuses on the legal aspects of collecting, storing, and using electronic data, including issues related to the chain of custody, technical standards, and procedural control [1, 4, 18]. Many studies emphasise the importance of harmonising national regulations with international standards to prevent legal uncertainty and improve the efficiency of judicial practice [2, 3, 19, 20].

Approaches to determining the admissibility of digital evidence differ across the literature. Some studies highlight the procedural conditions necessary for admissibility, while others focus on the technical reliability of the data and the application of digital forensic methods [21, p. 323; 22; 23]. International practice demonstrates the use of both open and closed information sources, along with standardised verification tools, which enhance the reliability of evidence across jurisdictions [11, p. 61, 24]. Furthermore, the integration of electronic evidence into judicial proceedings requires consideration of both human rights obligations and the technical standards for data preservation [20, 25–27].

Several publications note the insufficient integration of national legislation with digital forensics requirements, leading to gaps in assessing the admissibility and reliability of electronic evidence. Contradictions are also evident between the demand for effective criminal prosecution and the need to protect participants' rights, underscoring the need for balanced approaches and practical recommendations [7, 9, 10, 28–30].

The systematisation of research findings reveals several key areas for development:

a) Formalisation of legal criteria for evaluating digital evidence [15, p. 418, 16, p. 50–51];

b) Introduction of procedural controls to preserve data integrity [13, p. 20, 14, p. 220];

c) Development of methodological recommendations for practitioners in criminal proceedings [31–33];

d) International comparison of standards and practices [17, p. 16, 17, 34].

e) These areas underscore the need to improve legislation and practical procedures for handling digital information, forming a foundation for further research [31–33].

These areas underscore the need to improve legislation and practical procedures for handling digital information, providing a foundation for further research. However, there is a notable lack of comprehensive empirical studies that confirm the effectiveness of existing digital forensics procedures and tools. Many investigations are limited to theoretical analysis or case descriptions, indicating the need for data systematisation, comparative research, and the identification of regulatory weaknesses [5, 35–37].

Overall, the literature review demonstrates significant scholarly interest in digital evidence, the existence of contradictions between theory and practice, and the need for comprehensive recommendations that integrate national norms with international standards to enhance the reliability, legitimacy, and fairness of criminal proceedings [2, 3, 38, 39].

MATERIALS AND METHODS

The study was conducted in several stages to systematically analyse the regulatory framework for digital information and assess the criteria for the admissibility of electronic evidence in criminal proceedings.

Stage 1: Theoretical Review of Legal Frameworks. The first stage consisted of a comprehensive review of legal acts, regulations, and international standards governing the collection, storage, and use of digital materials. This review focused in particular on procedures for ensuring

data integrity, authenticity, and reliability in criminal proceedings [1, 4, 5, 9]. The analysis included national legislation from multiple jurisdictions, as well as international conventions, protocols, and standards such as ISO/IEC 27037:2012, Council of Europe guidelines, and the Second Additional Protocol to the Cybercrime Convention. This study focused on aligning forensic technical procedures with procedural requirements to protect participants' rights in criminal proceedings [20, 25].

Stage 2: Selection and Analysis of Scientific Literature. Scientific publications were identified using systematic search strategies across multiple databases. The databases included: Scopus and Web of Science – for their extensive coverage of peer-reviewed journals and high scientometric reliability; Google Scholar – for broad inclusion of scholarly articles, conference proceedings, and grey literature; SSRN and arXiv – for legal and technological preprints relevant to emerging practices in digital forensics [36, 39]; UIA Global Civil Society Database and SWGDE – for reports and guidelines from professional organisations specialising in digital evidence [23, 40].

The researchers selected these databases to ensure comprehensive coverage of peer-reviewed research, legal analyses, technical guidelines, and international best practices relevant to electronic evidence.

The selection of publications followed PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. The search strategy included keywords such as digital evidence, electronic evidence, e-evidence, cyber forensics, chain of custody, admissibility of digital materials, criminal proceedings, data integrity, international standards; inclusion criteria as publications from 2018–2025, peer-reviewed journal articles, books, professional reports, and international standards, works addressing legal, procedural, or technical aspects of digital evidence, studies in English, Ukrainian; exclusion criterias as publications unrelated to criminal proceedings or digital evidence, non-scholarly sources (e.g., news articles, blogs), duplicates and outdated materials.

Stage 3: Data Systematisation and Analysis. The researchers systematically categorised the retrieved publications and documents according to:

a) Jurisdiction – national vs international frameworks;

b) Type of digital evidence – open-source vs closed-source, AI-generated, cloud-based, or physical media [10, 29];

c) Procedural focus – collection, storage, admissibility, chain of custody;

d) Methodological approach – theoretical analysis, empirical studies, case law review [21, 22].

The researchers used content analysis to extract key themes, trends, gaps, and contradictions in the literature. A comparative legal approach enabled the evaluation of alignment between national regulations and international standards, as well as the assessment of practical compliance with digital forensics requirements [3, 11, 31]. The researchers then synthesised the results to identify criteria for admissibility, procedural safeguards, and recommendations for harmonising legislation across jurisdictions [7, 30].

This structured methodology ensured a transparent, reproducible, and comprehensive review of both legal and scientific perspectives on digital evidence, providing a strong foundation for subsequent analysis and recommendations.

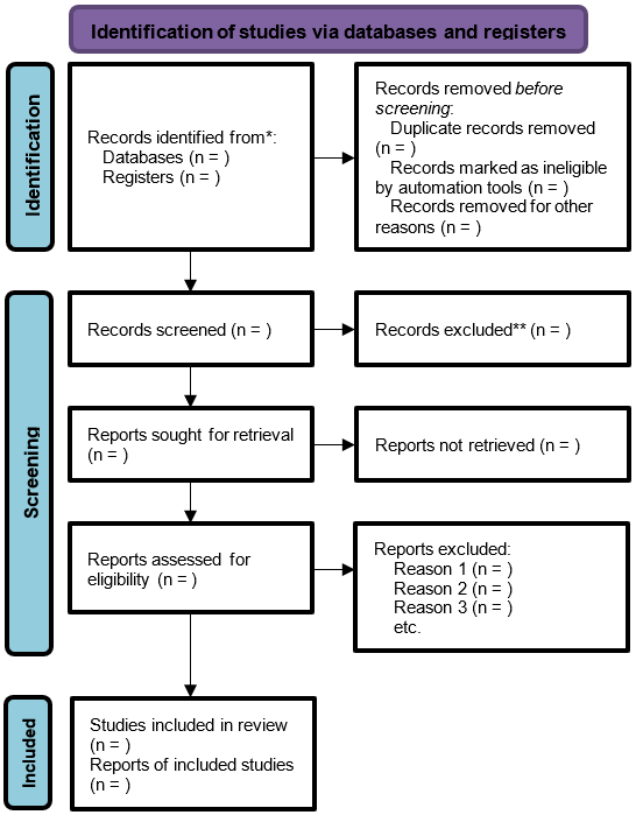

Figure 1 – PRISMA 2020 flow diagram [41]

The third stage involved the study of empirical data, including an analysis of judicial practice and

the results of the use of digital evidence in criminal cases, which made it possible to verify theoretical conclusions and identify the impact of violations of the chain of custody and procedures on the realisation of the right to a fair trial [5, 8, 9, 15, 29]. The researchers used quantitative and qualitative methods to process the data, including comparative analysis and the structuring and systematisation of information according to the criteria of admissibility, reliability, and integrity [30].

The methodology used enabled the establishment of a relationship among procedural standards, the technical requirements of digital forensics, and the practical aspects of using electronic evidence [18, 24, 42]. The study's structure allows other researchers to replicate the analysis using identical sources and approaches, thereby ensuring the reproducibility and reliability of the results [4, 10, 11].

Sample and Participants. The object of the study comprises criminal cases involving the use of digital evidence, as well as regulatory acts and judicial practice governing its use. The sample was selected to ensure the material's representativeness for analysing current approaches to the admissibility, reliability, and integrity of electronic data. The study includes court decisions from different jurisdictions, publications on digital forensics, and international standards, providing a comprehensive overview of the subject.

The sample is stratified: cases and sources are categorised by type of digital evidence, level of legal regulation, and nature of procedural violations. This stratification enables a thorough examination of both the theoretical and practical aspects of using electronic data, as well as the identification of patterns and typical challenges.

The number of materials and objects studied allows reliable conclusions to be drawn, reflecting the current state of regulatory control and practical approaches to working with digital information in criminal proceedings. The sampling method used ensures the reliability of the analysis and the reproducibility of the results by other researchers using similar criteria.

Instrument and Procedure. A combination of comprehensive methods was employed to collect and analyse data, ensuring a thorough examination of digital evidence and regulatory approaches to its admissibility. The main instruments used were content analysis of court decisions, comparative legal analysis of regulatory acts, and systematisation of scientific publications from the last five years. Content analysis enabled the identification of recurring errors in the collection, storage, and presentation of electronic data. It facilitated assessing the impact of procedural violations on the evidentiary value of the materials.

Comparative legal analysis enabled a detailed comparison of national and international standards, highlighted regulatory contradictions and gaps, and established overarching principles for the admissibility of digital evidence. The systematisation of scientific literature enabled the consolidation of existing approaches to digital forensics, the evaluation of the effectiveness of applied technologies and procedures, and the identification of areas requiring further research.

The empirical component of the study involved examining statistical data on the use of electronic evidence in criminal cases, as well as analysing instances of violations of the chain of custody and procedural requirements. The results were interpreted using qualitative analysis, facilitating the identification of patterns and formulation of generalised recommendations. The methods and tools applied ensure the study's reproducibility and enable other researchers to verify the conclusions when examining comparable materials.

Data Analysis. The collected data were subjected to both qualitative and quantitative analyses to ensure a comprehensive assessment of digital evidence and regulatory approaches to its admissibility. Qualitative analysis comprised content analysis of court decisions and scientific publications, systematisation of recurring patterns, and comparison of procedural standards with digital forensics practices. The data were coded according to key criteria, including admissibility, reliability, integrity, and compliance with procedural norms.

Quantitative analysis involved processing statistical information from court cases involving digital evidence. Correlation analysis was employed to identify relationships between procedural violations and reductions in the evidential value of electronic data. When appropriate, the researchers conducted factor analysis to identify the primary factors influencing the reliability and admissibility of digital information and reported the proportion of variance explained by each factor.

The results were interpreted within the context of a comparative analysis of national and international standards, enabling the identification of regulatory gaps and evaluation of the impact of technical and procedural practices on the effectiveness of criminal prosecutions and the protection of the right to a fair trial. The methodology applied ensures the reproducibility of the study and the reliability of conclusions when similar materials are re-examined.

RESULTS AND DISCUSSION

The analysis of the regulatory framework for digital evidence in criminal proceedings revealed notable inconsistencies and gaps in admissibility standards across different jurisdictions. In several countries, legislation specifies mandatory conditions for the use of electronic evidence, including the legality of data acquisition, compliance with the chain of custody, preservation of data integrity and authenticity, and proper documentation of all procedural stages [1, 20, 25, 28, 43, 44].

However, the researchers identified substantial gaps. There is a lack of uniform criteria for assessing the admissibility of digital materials. Some national provisions conflict with modern requirements of digital forensics, resulting in legal uncertainty and increased risks of challenges during judicial proceedings [6, 18, 22, 37]. Moreover, technical and procedural requirements are often poorly integrated: storage protocols and technical parameters often do not align with procedural deadlines or rules for presenting evidence in court, thereby compromising the evidential value of electronic data [5, 11, 31].

Comparative analysis of foreign practices highlights more structured approaches to digital evidence management. For instance, the European Union has developed harmonised criteria for admissibility that incorporate data quality, collection and storage procedures, and adherence to fair trial principles [2, 3, 14]. In the United States, Middle Eastern countries, and selected Asian jurisdictions such as Singapore and Azerbaijan, digital forensics models combine procedural safeguards with technical verification. These models emphasise compliance with the chain of custody, integrity control, the use of certified software, and thorough documentation, thereby enhancing reliability and mitigating the risk of rights violations during criminal proceedings [4, 15, 16, 45].

The study also revealed that the admissibility and reliability of digital evidence depend on both procedural and technical requirements. Procedural conditions include lawful data acquisition, recording all stages of collection and analysis, and ensuring the rights of defendants and other participants [1, 5, 13, 30]. Technical conditions include maintaining data integrity, accurately identifying information sources, using certified and verified software, and properly maintaining the chain of custody [4, 22, 34]. Adherence to these standards increases the probative value of digital evidence and reduces the likelihood of it being challenged in court.

Overall, the findings demonstrate that ensuring the legal validity of digital evidence requires a coordinated approach that integrates both procedural and technical safeguards. Proper organisation of the chain of custody and consistent procedural control at all stages—collection, transfer, storage, and processing—significantly enhances the credibility of electronic materials. Violations at any stage may compromise authenticity and diminish evidential weight [1, 4, 9, 22].

The international comparison shows that advanced practices include automated logging, multi-level access control, and standardised documentation procedures, ensuring a high level of legal protection for digital evidence. These practices facilitate transparency, accountability, and balance between investigative efficiency and protection of participants' rights [21, 24, 33, 46].

Table 1 – Key procedural and technical conditions for the admissibility and reliability of digital evidence

Type of conditions	Main requirement	Description	Source
Procedural	Legality of acquisition	Collection of information in accordance with legal norms	[1]
Procedural	Recording of all stages	Documentation of actions during collection, transfer and analysis	[5]
Procedural	Ensuring the rights of participants	Protection of the rights of defendants and other participants	[4]
Technical	Data integrity	Investigators and other authorised personnel must	[22]

Type of conditions	Main requirement	Description	Source
		not alter data during storage and processing.	
Technical	Source identification	Clear identification of the device and origin of the information	[22]
Technical	Storage chain	Tracking all actions with evidence	[5]
Technical	Software reliability	Use of certified and tested software	[45]

Notes: The table reflects a set of requirements that determine the admissibility and reliability of electronic materials.

Compiled based on an analysis of literature and practices of national and foreign criminal justice systems [1, 4, 9, 15, 22].

Table 1 presents a set of interrelated procedural and technical measures critical to ensuring the reliability, integrity, and legal validity of digital evidence. It highlights the key stages of control over the collection, storage, and processing of information, as well as requirements for the use of verified tools and certified software solutions. Compliance with these measures reduces the likelihood of challenges in court, ensures accurate documentation of case circumstances, and maintains a balance between the efficiency of criminal investigations and the protection of participants' rights [1, 4, 12, 22, 24].

Proper organisation of the digital evidence storage chain and the implementation of procedural controls are essential for maintaining both the integrity and legal significance of electronic materials. Any violations during collection, transfer, processing, or storage can undermine the authenticity of the information and diminish its evidential value. Effective procedural control ensures that every stage of handling digital materials is recorded, guarantees transparency of actions, and minimises the risks of judicial challenge [1, 5, 11, 30].

International practice demonstrates diverse approaches to organising the storage chain. In the United States and the United Kingdom, emphasis is placed on automated logging systems and strict access controls, allowing the complete history of digital evidence to be reliably tracked [9, 25]. In Germany and Ukraine, standardised documentation procedures, certified forensic software, and multi-level procedural control mechanisms are used to maintain high legal protection for evidence [4, 15]. In Asian jurisdictions such as Singapore, the UAE, Azerbaijan, and Pakistan, the chain of custody is integrated with digital forensics protocols and fair trial standards, thereby enhancing confidence in the legal reliability of electronic evidence [6, 31].

Table 2 summarises the key elements of the chain of custody and procedural controls applied in various countries, reflecting best practices for ensuring the integrity and admissibility of digital evidence. These elements include logging software, certified storage facilities, standardised documentation at all processing stages, verified forensic software, and regular procedural audits. Adoption of these measures contributes to the high legal significance of electronic materials and minimises the risk of challenges in judicial proceedings [2, 3, 33].

Table 2 – Key elements of the storage and procedural control chain in different countries

Country	Data Collection	Data Storage	Control and Audit	Tools Used	Source
United States	On-site recording and logging	Servers with restricted access	Automated auditing and reporting	Logging software, certified storage facilities	[1, 4, 38]
United Kingdom	Fixation and documentation	Centralised storage	Regular audits, access control	Proven software, electronic logs	[6, 19, 22]
Germany	Collection using certified software	Centralised storage	Multi-level verification	Certified tools and protocols	[2, 9]
Ukraine	Recording and documentation of all stages	Controlled server solutions	Audit and verification	Certified software, electronic journals	[3, 5, 15]

Country	Data Collection	Data Storage	Control and Audit	Tools Used	Source
UAE	Documentation and stage recording	Controlled server solutions	Validation and data verification	Certified software and transfer protocols	[21]
Pakistan	Recording and logging of actions	Centralised server systems	Access control and auditing	Proven tools, electronic logs	[30, 33]
Azerbaijan	Collection from verified sources	Centralised storage	Audit and verification	Certified software and transfer protocols	[11, 47]
Singapore	Recording and documentation of all stages	Centralised and cloud-based solutions	Regular auditing, access control	Proven digital platforms and security protocols	[4, 10, 24]

Notes: The table illustrates differences in approaches to organising the chain of custody and procedural controls of digital evidence across various countries. It highlights best practices for ensuring data integrity, legal reliability, and compliance with procedural standards.

Sources include national and international regulatory frameworks, technical protocols, empirical studies, and international standards (e.g., ISO/IEC 27037:2012, the Council of Europe Second Additional Protocol).

The diagram illustrating these elements enables a comparative assessment of compliance with international standards and highlights jurisdictions that implement advanced procedural and technical safeguards. Automated logging, multi-level access control, verified software, and standardised documentation enhance transparency, accountability, and adherence to fair trial principles. Countries with more structured systems—such as the United States, United Kingdom, Germany, UAE, and Singapore—demonstrate greater legal reliability of digital evidence, which guides improvements in jurisdictions with less formalised procedures [9, 21, 46].

Key elements of the storage and procedural control chain in these countries ensure the integrity of digital evidence through a combination of technological and organisational measures, including logging software and certified storage facilities. In the United States, the United Kingdom, Germany, Ukraine, Singapore, the United Arab Emirates, Pakistan, and Azerbaijan, all stages of data processing are recorded, and regular procedural controls are carried out, which increases the legal significance of the materials and reduces the risk of challenge. Visual representations of data in graphs allow you to compare the effectiveness of applying the storage chain and procedural control across different legal systems, as well as identify the most reliable approaches to ensuring the integrity of digital evidence.

To analyse the effectiveness of key elements of the digital evidence storage chain and procedural controls across different countries, a diagram is presented that shows indicators in three areas: data collection, information storage, and validation with integrity checks. The graphical representation allows us to identify differences in the practice of ensuring the reliability of digital materials and to assess the level of compliance of national procedures with international standards.

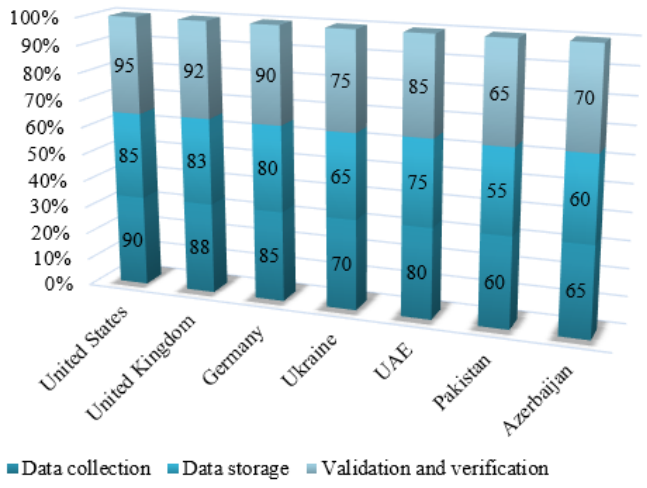

Figure 1 – Comparative indicators of elements of the chain of custody and procedural control of digital evidence in different countries (Prepared based on materials [1, 2, 3, 22, 29, 31, 32, 43])

Notes: The indicators reflect the level of implementation of key elements of the chain of custody and procedural controls for digital evidence across countries for 2018–2025.

The comparison results demonstrate differences in the level of organisation of the digital evidence

storage chain and procedural control between countries. The highest level of maturity is observed in the United States, the United Kingdom, and Germany, where comprehensive standards for automation, multi-level access control, and data verification have been fully implemented [16; 40]. Countries with developing systems, such as Ukraine, Pakistan, and Azerbaijan, rely on basic tools and procedures that require further standardisation, professional training, and integration with international standards [5, 15].

These indicators reflect a direct correlation between the degree of technical and organisational development of procedures and the legal force of digital evidence in court proceedings. Moreover, they highlight the need to harmonise national legislation with international protocols, including ISO/IEC 27037:2012 and the Council of Europe's Second Additional Protocol on electronic evidence [19, 38].

For a more detailed analysis of procedural control features, a comparison of individual audit and verification elements across countries is presented; this allows identification of the most developed control methods and highlights gaps in organisational practices that can affect the reliability, integrity, and legal admissibility of digital materials [4, 24].

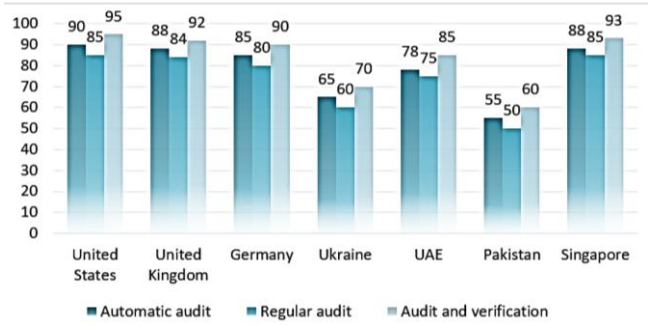

Figure 2 – Level of procedural control of digital evidence in different countries (prepared based on materials [1–4, 22, 29, 31, 32, 43])

Notes: The indicators reflect the level of implementation of key elements of the digital evidence storage and procedural control chain in different countries for 2018–2025.

Figure 2 illustrates the implementation of procedural controls over digital evidence, including automatic auditing, periodic verification, and systematic reporting. The data reflect the effectiveness of internal and external control mechanisms designed to prevent unauthorised changes, maintain integrity, and enhance the reliability of electronic information. Comparative analysis shows that the United States, the United Kingdom, Germany, and Singapore have high audit scores, reflecting robust mechanisms that ensure traceability and legal reliability. In contrast, lower scores in Ukraine, Pakistan, and Azerbaijan indicate the need to strengthen digital verification, forensic protocols, and professional training [21, 46, 47].

Assessing the consequences of procedural violations in the collection, storage, processing, and presentation of digital evidence is critical for protecting the right to a fair trial. Non-compliance with procedural control standards can lead to alteration or loss of information, compromise the probative value of evidence, and affect judicial outcomes [1, 5, 48].

Internal and external audits, as well as verification procedures, are particularly important because their effectiveness directly determines the reliability and admissibility of digital materials while safeguarding participants' rights in criminal proceedings. Observed practices show that highly developed systems in the US, UK, and Germany reduce disputes over evidence authenticity, whereas developing jurisdictions face increased legal risks due to weaker procedural controls [4, 22].

Based on these findings, it is necessary to develop comprehensive guidelines for proper handling of electronic evidence, covering standards for data collection, processing, presentation, audit, and verification. Implementation of such guidelines enhances the reliability of evidence, ensures procedural transparency, and harmonises practices among investigators, forensic experts, and judges [6, 24].

Investigators, forensic experts, and judges should give particular attention to practical methodological tools that document, verify, and protect digital data against unauthorised changes. Adoption of these recommendations strengthens confidence in digital evidence, mitigates risks of procedural violations, and contributes to the consistent application of international standards, including ISO/IEC 27037:2012 and the Council of Europe's Second Additional Protocol on electronic evidence [19, 38].

The rapid proliferation of digital technologies has fundamentally transformed the landscape of

criminal proceedings, making electronic evidence an increasingly central component of investigations and trials. This study analysed the regulatory framework governing digital information in criminal proceedings, focusing on the admissibility, reliability, and integrity of electronic evidence. The research addressed key questions on procedural standards, technical requirements, the chain of custody, and compliance with international standards, aiming to identify regulatory gaps and propose recommendations to harmonise legislation and judicial practice.

Summary of Key Findings. Our results demonstrate that the reliability and legal significance of digital evidence heavily depend on the presence of comprehensive procedural and technical standards. Procedural measures—including the legality of information acquisition, documentation of all stages of collection, and protection of participants' rights—are essential for ensuring compliance with fair trial requirements [1, 4, 5, 43]. Technical measures, such as maintaining data integrity, accurate source identification, implementing secure storage chains, and using certified software, play an equally critical role in preserving evidential value and preventing challenges in court [2, 22, 45].

Comparative analysis across jurisdictions revealed significant differences in the application of these standards. Countries with advanced regulatory systems, such as the United States, the United Kingdom, Germany, and Singapore, demonstrate robust integration of procedural safeguards and technical controls, including automated logging, multi-level verification, and standardised documentation practices. These measures collectively strengthen the reliability, admissibility, and integrity of digital evidence, supporting the effectiveness of criminal investigations while safeguarding participants' rights [2–4, 6].

Conversely, in countries such as Ukraine, Pakistan, and Azerbaijan, regulatory gaps were observed, including inconsistencies between procedural deadlines and technical requirements, limited standardisation of collection methods, and insufficient integration of digital forensics into judicial practice. These gaps increase the likelihood of violations of the chain of custody and diminish the probative value of electronic materials [5, 29, 32, 33]. Empirical data from court cases in these jurisdictions further confirmed that procedural or technical violations directly affect the outcomes of criminal proceedings, often leading to disputes over admissibility and potential exclusion of crucial evidence.

The study also highlights that aligning national regulations with international standards, such as ISO/IEC 27037:2012 and Council of Europe guidelines, is a key factor in increasing both the legal reliability and the cross-border applicability of digital evidence [1, 24]. Jurisdictions that actively implement these standards demonstrate higher consistency in evidence handling, stronger protection of participants' rights, and lower risk of procedural challenges.

Overall, the findings emphasise the need for a harmonised framework that integrates procedural controls, technical safeguards, and international best practices. Developing clear methodological guidelines for investigators, forensic experts, and judicial authorities can reduce risks of evidence tampering, improve documentation, and ensure that digital evidence is both legally admissible and technically reliable across different legal systems.

Interpretation and Comparison with Existing Literature. The study's findings largely corroborate prior research indicating that gaps in national regulation compromise the legal significance of digital evidence [3, 29]. Consistent with existing literature, the analysis highlights the critical importance of the chain of custody, procedural documentation, and the use of certified technical tools to ensure the reliability and admissibility of electronic materials [1, 22]. Additionally, the study confirms that standardised auditing and verification mechanisms, particularly when integrated with automated logging systems, enhance evidential reliability and mitigate human error, reinforcing conclusions from previous international studies [36, 39, 49].

Some unexpected findings also emerged. While earlier studies emphasised primarily technological solutions, such as certified software and AI-assisted verification [32, 45], our results demonstrate that organisational measures—such as procedural documentation, cross-checks, and regular audits—are equally critical for ensuring admissibility. In jurisdictions with advanced technical capabilities but weaker procedural oversight, digital evidence may still face challenges in court due to incomplete or inconsistent procedural recording. This finding underscores that technology alone cannot guarantee reliabil-

ity; an integrated approach combining procedural rigour and technical safeguards is necessary.

Furthermore, the study extends existing research by providing a systematic, cross-jurisdictional analysis of both procedural and technical measures, illustrated through detailed tables of best practices and storage chain mechanisms. Unlike prior studies, which often examined technical or procedural aspects in isolation [4, 5], this research integrates both dimensions, offering a comprehensive perspective on the factors that influence the admissibility, reliability, and legal significance of digital evidence across diverse legal systems.

Limitations. Despite the comprehensive approach, the researchers acknowledge certain limitations.

First, the study relies on published court decisions and scientific literature, which may introduce publication bias. Courts and law enforcement agencies do not publicly report all cases involving digital evidence, which may limit the representativeness of the sample.

Second, although the research spans multiple jurisdictions, the selection of countries was influenced by data availability and may not fully reflect global practices.

Third, the researchers primarily derived the empirical data from qualitative content analysis and secondary sources; future researchers could incorporate primary quantitative datasets or experimentally validate digital forensic methods to strengthen the generalisability of the findings.

Finally, technological tools and standards are evolving rapidly, so some findings may require periodic updates to remain current with emerging practices.

Contribution and Scientific Novelty. This study makes several important contributions to the scientific field of criminal justice and digital forensics. Firstly, it develops a comprehensive framework that links procedural and technical requirements for the admissibility, reliability, and integrity of digital evidence, synthesising best practices from multiple jurisdictions. Secondly, it applies a systematic methodology that combines content analysis, comparative legal analysis, and the empirical examination of court cases, ensuring reproducibility and transparency. Thirdly, the study identifies critical gaps in existing legislation and practice, particularly in countries with developing digital forensics standards, and proposes evidence-based guidelines for harmonisation with international norms.

The novelty of the work lies in integrating procedural, technical, and comparative perspectives, providing a cross-jurisdictional synthesis previously missing in the literature. By combining qualitative and quantitative assessments with a focus on chain-of-custody compliance, the research highlights practical steps to enhance the probative value of electronic evidence while safeguarding participants' rights. This dimension has not been fully explored in prior studies [1, 4].

Practical Implications. The study has several practical implications. Lawmakers can use the findings to refine regulations on electronic evidence, incorporating clear standards for collection, storage, and verification. Judicial authorities can adopt structured audit and logging practices to ensure the integrity of digital materials. Legal practitioners, including prosecutors and defence attorneys, can benefit from understanding both procedural and technical requirements that affect admissibility and reliability. The results also support training programs for digital forensic experts, emphasising that procedural documentation is as important as technological tools.

Furthermore, the findings provide a roadmap for international harmonisation, suggesting that countries with weaker regulatory frameworks can adopt best practices from jurisdictions with high compliance standards, including multi-level verification, certified software, and automated logging systems. Such harmonisation is crucial for cross-border investigations, where inconsistencies in the admissibility of evidence can hinder cooperation and reduce the effectiveness of prosecution [2, 3].

Based on the findings of this study, several recommendations are proposed to strengthen the collection, storage, and use of digital evidence in criminal proceedings. Firstly, there is a critical need to standardise procedural requirements. Legislators should formalise documentation procedures, clearly define the responsibilities of personnel handling electronic evidence, and require personnel to consistently record every stage of evidence collection, transfer, and analysis. This formalisation will help prevent procedural gaps and enhance the legal reliability of digital materials in court.

Secondly, the study highlights the importance of integrating technological safeguards into existing legal frameworks. Legislators should mandate the use of certified and verified software, automated logging systems, and secure storage solutions to minimise the risk of human error and preserve the integrity and authenticity of digital evidence. Such measures ensure that electronic materials remain reliable and legally admissible, even in complex or cross-border investigations.

Thirdly, training and capacity-building are essential for effective implementation. Judicial staff, forensic experts, and legal practitioners should receive comprehensive instruction on both procedural and technical aspects of digital evidence. This training should cover chain-of-custody management, verification protocols, and best practices for using digital forensic tools, allowing professionals to maintain compliance with established standards and improve the quality of judicial outcomes.

Another key recommendation is the harmonisation of national regulations with international standards. Countries with underdeveloped legal frameworks should adopt globally recognised guidelines, such as ISO/IEC 27037:2012 and the Council of Europe recommendations, to align domestic practice with international norms. This harmonisation facilitates cross-border cooperation, ensures consistent assessment of digital materials, and strengthens confidence in electronic evidence across different legal systems.

Finally, the study emphasises the need for regular monitoring and evaluation of digital evidence procedures. Continuous auditing, verification, and review mechanisms should be established to detect and address procedural lapses promptly. Routine assessments will enhance transparency, maintain the integrity of digital materials, and increase trust in the judicial process, ensuring that electronic evidence consistently meets both technical and procedural standards.

Together, these recommendations provide a comprehensive roadmap for improving the management of digital evidence, balancing technological reliability with procedural fairness, and promoting the consistent application of best practices in criminal proceedings.

CONCLUSIONS

The strength of regulatory control largely determines the effective use of digital information in criminal proceedings, the transparency of procedural oversight, and strict compliance with audit and verification standards. This study demonstrated that in countries with well-developed legal and technological infrastructures, such as the United States, the United Kingdom, Germany, and Singapore, electronic evidence is highly admissible and reliable. Conversely, in states with limited regulation, including Ukraine, Pakistan, and other jurisdictions, gaps in legal frameworks increase the risk of procedural violations, compromise the integrity of digital materials, and may negatively affect the fairness of judicial outcomes [1, 4].

This study fully achieved its objective: conducting a comprehensive assessment of the regulatory framework governing digital information in criminal proceedings and developing recommendations to improve legal and procedural standards. The study confirmed that procedural requirements, including legality of acquisition, documentation of all stages, and protection of participants' rights, are essential for admissibility. Technical requirements, such as data integrity, source identification, proper storage chains, and the use of certified software, are equally critical for maintaining reliability. These findings provide a clear answer to the first research question regarding the criteria for admissibility of digital evidence.

In response to the second research question on the interaction between procedural rules and digital forensics, the study found that chain-of-custody procedures, auditing procedures, and automated verification systems significantly enhance evidential value. The third question, regarding the consequences of breaches in procedural control, was addressed by demonstrating that violations in collection, transfer, or storage stages diminish the probative value of digital materials and may compromise the right to a fair trial. The study confirmed that balancing the effectiveness of criminal prosecution with participants' rights requires integrated legal and technological standards.

Prospects for further research include the development of detailed methodological guidelines for law enforcement and judicial authorities, analysis of international case studies, and the creation of a harmonised legal and technological framework for digital evidence applicable at both national and international levels. Future studies should also explore integrating emerging technologies,

including artificial intelligence, blockchain, and cloud-based systems, to further enhance the security, reliability, and admissibility of electronic evidence. These steps will contribute to a more consistent, transparent, and effective criminal justice system globally.

Suggestions for future research. To improve the effectiveness of regulatory control and the use of digital information in criminal proceedings, policymakers should develop a comprehensive set of methodological recommendations for all participants in judicial proceedings, including investigators, experts, and judges. These recommendations should cover standards for the collection, processing, storage, and presentation of digital evidence, as well as audit and verification procedures.

Researchers should study international experience in the use of digital evidence and identify best practices that can be adapted to national legislation. Another promising area is the introduction of digital forensics technologies and artificial intelligence tools to automate the verification and analysis of electronic data.

In addition, researchers should assess the impact of new technological solutions on the right to a fair trial and develop uniform standards to ensure the compatibility and reliability of digital evidence in transnational criminal investigations.

REFERENCES

1. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs, 3*(5), 795–805. doi: 10.71317/rjsa.003.05.0375

2. Politova, A., & Chekhlai, T. (2025). Admissibility of Digital Evidence in Criminal Proceedings: An Analysis of Case Law. *Vìsnik Marìupol's'kogo Deržavnogo Unìversitetu Serìâ Pravo, 15*(29), 104–115. doi: 10.34079/2518-1319-2025-15-29-104-115

3. Romaniuk, V. V., & Ablamskyi, S. Y. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law And Safety, 93*(2), 140–150. doi: 10.32631/pb.2024.2.13

4. Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International Digital Investigation, 45*, 301554. doi: 10.1016/j.fsidi.2023.301554

5. Fomina, T. H., & Rachynskyi, O. O. (2023). Electronic evidence in criminal proceedings: problematic issues of theory and practice. *Bulletin of Kharkiv National University of Internal Affairs, 102*(3 (Part 2)), 207–220. doi: 10.32631/v.2023.3.43

6. Lasagni, G. (2025). Admissibility of digital evidence. In *Cambridge University Press eBooks* (pp. 126–152). doi: 10.1017/9781009049771.007

7. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1). doi: 10.1093/cybsec/tyac014

8. Brayne, S. (2018). The criminal law and law enforcement implications of big data. *Annual Review of Law and Social Science, 14*(1), 293–308. doi: 10.1146/annurev-lawsocsci-101317-030839

9. Brown, E. K. (2022). Digital forensic and distributed evidence. *Advances in Multidisciplinary & Scientific Research Journal Publication, 1*(1), 357–362. doi: 10.22624/aims/crp-bk3-p57

10. Kattan, M. S. A. (2024). Digital Justice "Model of the United Arab Emirates". *Revista De Gestão Social E Ambiental, 18*(1), 04945. doi: 10.24857/rgsa.v18n1-091

11. Peake, J. (2024). Challenges of using digital evidence for war crimes prosecutions: availability, reliability, admissibility. *AJIL Unbound, 118*, 57–61. doi: 10.1017/aju.2024.5

12. Figursky, V. M. (2023). E-Evidence in Criminal Proceedings. *Galician Studies Law Sciences, 4,* 97–105. doi: 10.32782/galician_studies/law-2023-4-14 (in Ukrainian).

13. Juszczak, A., & Sason, E. (2023). The use of electronic evidence in the European area of freedom, security, and Justice: An introduction to the new EU Package on e-Evidence. *Eucrim – the European Criminal Law Associations Forum, 18*(2), 182–200. doi: 10.30709/eucrim-2023-014

14. Kostenko, & Ghaziani. (2024). Admissibility of illegally obtained e-evidence: A critical study of EU law and the precedents of the European Court of Human Rights/Ammissibilità delle prove elettroniche ottenute illegalmente: uno studio critico del diritto dell'UE. *European Journal of Privacy Law & Technologies, 2*, 205–220. doi: 10.57230/ejplt242ovkvag

15. Kozytska, O. (2020). On the Concept of Electronic Evidence in Criminal Proceedings. *Juridical Scientific and Electronic Journal, 8*, 418–421. doi: 10.32782/2524-0374/2020-8/103

16. Kvashuk, O. D. (2025). The Use of Electronic Evidence in Criminal Proceedings. Central *Ukrainian Journal of Law and Public Administration, 2*, 50–56. doi: 10.32782/cuj-2025-2-5 (in Ukrainian).

17. Vedwal, A. (2023). Admissibility of digital evidence in cybercrime investigations. *SSRN Electronic Journal*. doi: 10.2139/ssrn.4443356

18. Bagus, R. (2025). Analysing the Legal Frameworks Governing Digital Evidence Collection in Cross-Border Cybercrime Investigations. *International Journal of Criminal Law and Criminal Justice (Ijclcj), 3*(2), 1-7

19. Council of Europe. (n. d.). Second Additional Protocol to the Cybercrime Convention on enhanced cooperation and disclosure of electronic evidence (CETS No. 224). Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol

20. Cybercrime Convention Committee (T-CY). (2021). Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Explanatory Report. Retrieved from https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a48e4b%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

21. Elsharkawy, M. H. (2025). Digital Evidence before the International Criminal Court. *Journal of Law and Emerging Technologies, 4*(1), 323–426.

22. Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS ONE, 20*(9), 0331683. doi: 10.1371/journal.pone.0331683

23. Scientific Working Group on Digital Evidence (SWGDE). (2026). SWGDE. Retrieved from https://www.swgde.org/documents/current-documents/

24. Franssen, V., Tosza, S., Erbežnik, A., Svantesson, D., Osula, A., Robinson, G., De Saint Guilhem, C. D., Lasagni, G., Tropina, T., Christakis, T., Aguinaldo, M. a. L., De Hert, P., Careel, S., Verbruggen, F., Kasper, A., Laurits, E., Sogomonjan, M., Brodowski, D., McIntyre, T. J., & Bilgiç, S. (2025). The Cambridge Handbook of Digital Evidence in Criminal Investigations. In *Cambridge University Press eBooks*. doi: 10.1017/9781009049771

25. Congress.gov. (1975). 1926 Public Law 93-594-Jan. 2, 1975. Retrieved from https://www.congress.gov/93/statute/STATUTE-88/STATUTE-88-Pg1926-2.pdf

26. Pertsova-Todorova, L. (2020). 'Electronic evidence' during a search. *Entrepreneurship Economy and Law, 6*, 243–247. doi: 10.32849/2663-5313/2020.6.41 (in Ukrainian).

27. Shulhan, I. (2023). Electronic evidence as an effective tool of proving in criminal proceedings. *Lviv Politechnic Publishing House* (in Ukrainian).

28. Ablamskyi, S. Y., Havryliuk, L. V., Drozd, V. G., & Nenia, O. V. (2021). Substantial violation of human rights and freedoms as a prerequisite for inadmissibility of evidence. *Justicia, 26*(39), 47–56. doi: 10.17081/just.26.39.4819

29. Avdeeva, G., & Żywucka-Kozlowska, E. (2023). Problems of using digital evidence in criminal justice of Ukraine and the USA. Theory and Practice of Forensic Science and Criminalistics, 30(1), 126–143. doi: 10.32353/khrife.1.2023.07

30. Hossain, B. (2023). Digital Evidence in Foreign Jurisdiction and Quality of Justice. *ELCOP Journal on Human Rights, 1,* 143–159.

31. Matis, J. (2025). Digital evidence and its use for criminal proceedings. *Analytical and Comparative Jurisprudence, 3*(3), 121–126. doi: 10.24144/2788-6018.2025.03.3.19

32. Metelev, O. (2023). Digital Evidence in Criminal Procedure: Typological Characteristic. *Herald of Criminal Justice, 1–2,* 42–53. doi: 10.17721/2413-5372.2023.1-2/42-53

33. Nazir, S., Asif, M., & Khan, A. U. A. (2025). Digital Evidence in Pakistan: A doctrinal assessment of admissibility and reliability in criminal trials. *Advance Social Science Archive Journal, 4*(1), 1941–1951. doi: 10.55966/assaj.2025.4.1.0107

34. Selim, A., & Ali, İ. (2024). The role of digital forensic analysis in modern investigations. *Journal of Emerging Computer Technologies, 4*(1), 1–5. doi: 10.57020/ject.1445625

35. Prysiazhniuk, I. (2023). Use of digital evidence in the criminal process: some issues of privacy protection. *Visegrad Journal on Human Rights, 5*, 81–88. doi: 10.61345/1339-7915.2023.5.11

36. Singh, S., & Devi, L. (2025). Reliability and admissibility of AI-Generated Forensic Evidence in criminal trials. *arXiv (Cornell University).* doi: 10.48550/arxiv.2601.06048

37. Bharati, R., Khodke, P. G., Khadilkar, C. P., & Bawiskar, S. (2024). Forensic Bytes: Admissibility and challenges of digital evidence in legal proceedings. *SSRN Electronic Journal*. doi: 10.2139/ssrn.4896874

38. ISO. (2012). ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from https://www.iso.org/standard/44381.html?__cf_chl_f_tk=YNTXaagfLzznnK1XurmErq7mlEVl2ubB3WDcHlMYHKU-1783076822-1.0.1.1-0kL_GqCj0y7MWugstgnUam8JMtl7P.LO5YLhMTXm08g

39. Yin, Z., Wang, Z., Xu, W., Zhuang, J., Mozumder, P., Smith, A., & Zhang, W. (2025). Digital Forensics in the Age of Large Language Models. *arXiv:2504.02963*

40. Global Civil Society Database. (n. d.). International Organisation on Computer Evidence (IOCE). Retrieved from https://uia.org/s/or/en/1100029648

41. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ, 372*, 71. doi: 10.1136/bmj.n71

42. Akhmetov, A. T., Bekisheva, S. D., Syrbu, A. V., & Kainazarova, D. B. (2018). Retrospective Review of Information Technologies in the Criminal Code of Kazakhstan. *Journal of Advanced Research in Law and Economics, 9*(5), 1545-1550,

43. Akhtyrska, N., & Kostiuchenko, O. (2022). Procedural and organisational aspects of electronic evidence collection during international cooperation. *Uzhhorod National University Herald Series Law, 2*(72), 192–198. doi: 10.24144/2307-3322.2022.72.64

44. Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice, 61*(6), 761–770. doi: 10.1016/j.scijus.2021.10.003

45. Miller, C. M. (2022). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International Synergy, 6,* 100296. doi: 10.1016/j.fsisyn.2022.100296

46. Fatiha Ressa, F. (2025). Digital evidence and its legitimacy in comparative systems. *The International Tax Journal, 52*(6), 4455–4465.

47. Mikayılov, A. S. O. (2023). Innovations in the Criminal Procedure of the Republic of Azerbaijan: Prospects for the implementation of modern methods and technologies in the work of specialists. *Futurity Economics&Law*, 190–208. doi: 10.57125/fel.2023.12.25.12

48. Stoykova, R. (2024). A new right to Procedural accuracy: a governance model for digital evidence in criminal proceedings. *Computer Law & Security Review, 55*, 106040. doi: 10.1016/j.clsr.2024.106040

49. Asgarova, M. P. (2025). AI in Big Data in Criminal Investigation: Procedural Safeguards and Human Rights Risks. *Jurnal Cita Hukum, 13*(3).