American Journal of Society and Law (AJSL)

ISSN: 2835-3277 (ONLINE)

VOLUME 5 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Society and Law (AJSL)

Volume 5 Issue 1, Year 2026
ISSN: 2835-3277 (Online)
DOI: https://doi.org/10.54536/ajsl.v5i1.7211
https://journals.e-palli.com/home/index.php/ajsl

The Use of Digital Evidence in Criminal Proceedings

Novera Bhatti[1*]

Article Information

Received: November 20, 2025

Accepted: March 05, 2026

Published: March 30, 2026

Keywords

Admissibility, Chain of Custody, Criminal Proceedings, Digital Evidence, Digital Forensics

ABSTRACT

The use of digital evidence has become an essential part of contemporary criminal proceedings as it has radically transformed the way justice systems investigate, prosecute as well as adjudicate crime. The ever-increasing data volume created by computers, mobile devices, cloud computing systems, and Internet of Things devices has presented both unmatched possibilities in the crime detection process and very difficult challenges to the legal systems that are in place to regulate the flow of such data to be collected, stored, analyzed and presented. The current evidentiary and procedural systems - designed to work in a physical evid25 E. Jackson Blvd, Chicago, IL 60604, USA.ence world - are, in turn, becoming stretched by the instability, complexity, and location-based fluidity of digital information, introducing systemic threats to procedural fairness and the presumption of innocence. The article goes beyond a pure theoretical and conceptual discussion of the digital evidence at the criminal proceedings level, relying on the digital forensics literature, evidence law, and the theory of governance. It critically analyzes admissibility norms in the leading legal systems, models of the forensic process and regulatory difficulties of new forms of evidence. The paper suggests a four-pillar governance framework such as legal standards, forensic integrity, chain of custody, and fairness and rights with the underlying international harmonisation and technological adaptation mechanisms. This article posits that the digital evidence needs not only technical enhancement of the forensic approach, but a deliberate redefinition of the regulatory structure that is adaptable to the technological advancement without losing the basic principles of criminal justice fairness, accuracy, and protection against false conviction.

INTRODUCTION

The digitization of the modern world has revolutionized the landscape of evidencing criminal justice systems not only in a profound and yet to be fully comprehended way. Each touch with a digital device - a smart phone, a laptop, a smart home appliance, a cloud storage application, a financial platform - creates data that in a criminal investigation may serve as evidence of the commission of an offence, identity of a perpetrator, location of a suspect, or a criminal network. In case of cybercrime and financial fraud as well as terrorism, homicide and sexual exploitation, as Casey (2011) noted, digital evidence is now being found in virtually all categories of serious criminal offence. The ability of law enforcement agencies to gather, store, and examine computer-related evidence has become a major factor in the successful criminal prosecution; the ability of courts to assess and sentence based on computer-related evidence has become a major factor in determining the fairness of criminal proceedings.

The issue of concern that gives rise to this paper is the increasing disparity between technological advances and the ability of the legal system to regulate the application of digital evidence in criminal cases. The current evidentiary doctrine and forensic practice were established in a society of physical evidence of fingerprints, documents, and witness testimony, and their adjustment to the unique properties of digital evidence has been selective, ad hoc, and responsive. According to Stoykova (2021), the unaddressed risks to fairness and the presumption of innocence associated with the treatment of digital evidence in the framework of criminal procedure systems are systemic because of the specific treatment of digital evidence. Leroux (2004) reported the basic issues of legal admissibility of electronic evidence 20 years ago but a lot of the jurisdiction and normative gaps of the issues were yet to be fully addressed as observed during that early period of digital evidence research. The rapid increase of digital transformation - through the advent of cloud computing, the Internet of Things, artificial intelligence, and blockchain technology as the latest sources of criminal evidence - has brought to the fore the necessity to fill these gaps like never before.

There are four major objectives of this article. Originally, it formulates an intellectual explanation of digital evidence its types, features, and peculiarities of evidentiary problems based on the developed forensic and legal literature. Second, it critically looks at admissibility systems and forensic processes models that are used to evaluate the application of digital evidence in criminal proceedings and the structural constraints therein. Third, it promotes a comparative theoretical study of the normative standards which must guide the admissibility of digital evidence in the legal systems. Fourth, it suggests a governance model based on four mutually supportive pillars, namely, legal standards, forensic integrity, chain of custody, and the safeguarding of fairness and basic

[1] DePaul College of Law, 25 E. Jackson Blvd, Chicago, IL 60604, USA
[*] Corresponding author's e-mail: novera.bhatti1998@gmail.com

rights. The article is hypothetical and theoretical in nature - it does not produce or interpret empirical evidence but instead summarizes the existing literature of the scholarship into a consistent normative structure of a regulatory reform.

The importance of this question goes far beyond the practical issues of police departments or crime laboratories. When a criminal justice system wrongfully convicts a person due to the inadequacy or lack of understanding of digital evidence, it is one of the most severe types of injustices that can ever happen to a person (Goodison *et al.,* 2015; Stoykova, 2024). The current academic research on the matter of digital evidence governance has made significant progress since the original analysis of admissibility issues by Leroux (2004) and more recent works by Stoykova (2021; 2024) in her more normative analysis of deficiencies in fairness and by Park and Jeong (2026) in her technical design of the blockchain-based storage of custody have provided significant additional conceptual material with which to regulate this matter. Nevertheless, there is no contribution to date that has been able to integrate the developments into a unified four dimensional governance architecture that deals with legal standards, forensic integrity, chain of custody and fundamental rights as interdependent as opposed to discrete regulatory requirements. This article fills that gap. The article will be structured in the following way: Section 2 will include thematic literature review of four sub-domains; Section 3 will include the description of the methodology; Section 4 will include the results and discussion that will include the comparative analysis of admissibility as well as introduction of the suggested governance framework and the implications thereof; a conclusion will be made in Section 5, and the priorities of future research will be identified

LITERATURE REVIEW

Digital Evidence Evolution and Conceptualisation

Digital evidence and digital forensics as an academic field of study became a reality in the late 1980s and 90s as a result of the popularization of personal computers as a means of committing crimes and as a response to the need by law enforcement agencies to have principled means of retrieving and studying digital evidence. Pollitt (2013) gives a historical background of the establishment of digital forensics as a discipline, the evolution of informal methods of law enforcement to the establishment of standardised procedures, professional bodies, and even academic research courses. Definitional limits of digital evidence have dramatically broadened during this time-span: a range of data saved on the drives of personal computers to network traffic, content stored on mobile devices, cloud-based storage, and the ever-expanding range of output of IoT and smart devices (Garfinkel, 2010).

Casey (2011) has given the largest theoretical explanation of digital evidence which he defines as any probative information that has been stored or transferred electronically that can be utilized at trial by any party to a court proceeding. This definition not only describes that digital data are stored and transmitted as a form of digital evidence, but also locates digital evidence on the normative plane of a legal process instead of perceiving it as a strictly technical one. Angel *et al.* (2024) adopt a more law-specific conceptualisation of digital evidence as a tool of evidence used in criminal proceedings and situate its applicability within the legal structures of the formal procedures of the evidence law. Dmitrieva and Pastukhov (2023) present a comparative study of the idea of electronic evidence in criminal legal procedure in various legal traditions and find significant differences in definitions of the concept both in the civil law and common law systems, which exacerbate the cross-border collaboration in the evidence process.

The academic literature constantly defines a collection of peculiar features distinguishing a digital evidence based on the traditional physical evidence and create its major legal and forensic issues. Digital evidence is volatile, it can be changed or destroyed quickly, deliberately or accidentally, and leave no physically visible evidence. It can also be reproduced with ease and no clear distinction between the original and the copy thus casting fundamental concerns of authenticity and integrity (Arshad *et al.,* 2018). It is usually large in volume, and it cannot be processed manually in large volumes that may be challenging to assess by the courts and other people in the legal profession. And it is often spread over various devices, jurisdictions and service providers in a manner that makes it difficult to access lawfully and rebuild it forensically (Casino *et al.,* 2022). Another category of evidence quickly gaining momentum as a distinct problem demanding specific governance solutions that go beyond those sufficient in the context of traditional digital data is AI-generated and AI-analysed evidence such as deep fake detectives, predictive analytics reports, and automated pattern-recognition results (Garfinkel, 2010; Horsman, 2019). The table 1 below outlines in a structured manner the major types of digital evidence as they are faced in the criminal proceedings.

Table 1: Categories of digital evidence in criminal proceedings functions and challenges

Category of Digital Evidence	Description and Sources	Evidentiary Function	Key Regulatory and Forensic Challenges
Computer-Stored Data	Stored in hard drives or solid-state devices Files, documents, databases, emails, and spreadsheets.	Authorship identification; deleted files recovery; metadata that contains the history of creation and modification.	Easily volatile digital data; it can become contaminated during seizure; the vulnerability of the chain of custody (Casey, 2011; Arshad *et al.,* 2018)

Network and Internet Data	Internet protocol logs, web logs, email logs, social media logs, server logs, and communication logs.	Proving that there was co-conspirators; proving that there was the establishment of digital presence at a place or time.	Jurisdiction barrier across borders; encrypted information; changing IP addresses; data destruction in real time (Casino *et al.,* 2022; Leroux, 2004).
Mobile Device Evidence	SMS, call history, and GPS street address information, application data, photos, and content of messaging applications.	Tracking of locations; reconstructing communications in a criminal case; establishment of timeline in a criminal case.	Encryption of the device; proprietary operating systems; remote wipe feature; warrant (Goodison *et al.,* 2015; Novak, 2020)
Cloud-Based Evidence	Information saved in the environment of third-party servers: emails, documents, backup, collaboration platform records.	Retrieval of data that is not locally present; multi-device activity records that are synchronised are available.	Complexity of jurisdiction; barriers to cooperation between providers; conflict of data sovereignty (Ruan *et al.,* 2013; Quick and Choo, 2014)
IoT and Smart Device Data	Home records on smart, Health records on wearables, vehicle records on telematics, appliance activity records.	The corroboration of the environment and behaviour; the presence of suspects at the scenes; timeline.	Lack of standardisation of data between providers; proprietary structure; insufficient legal structures; risk of privacy invasion (Losavio *et al.,* 2016; Garfinkel, 2010)
Blockchain and Distributed Ledger Records	Records of cryptocurrency transactions, records of smart contract execution,data of an immutable distributed ledger.	Following the illegal monetary transactions; developing transactional relationships; delivering tamper-evident audit trails	The problem of pseudonymity; the technical complexity of courts; the inability to trace cross-chain (Tsai *et al.,* 2021; Park and Jeong, 2026)

Source: Synthesised from Casey (2011); Arshad et al. (2018); Casino et al. (2022); Leroux (2004); Ruan et al. (2013); Quick and Choo (2014); Goodison et al. (2015); Novak (2020); Losavio et al. (2016); Garfinkel (2010); Tsai et al. (2021); Park and Jeong (2026)

Standards of Admissibility and Frameworks of Evidentiary

There is a complicated combination of legislative regulations, the principles of common law, and forensic practices that determine the admissibility of digital evidence in criminal proceedings and differs considerably across jurisdictions. Leroux (2004) gives the comparative analysis of the legal admissibility of electronic evidence that is based on authenticity, integrity and reliability as the three major criteria used in a variety of major legal systems and reports on the considerable variations in the operationalisation of the criteria in various procedural settings. The most detailed modern treatment of the issue of electronic evidence admissibility by Mason and Seng (2021) covers both the legal criteria that constitute the substantive aspect of the issue and the procedural process by which digital evidence is presented, objected to, and discussed in a court of law.

In common law jurisdictions, digital evidence is usually evaluated by the standards of relevance, authenticity, reliability, and the lack of undue prejudice. Novak (2020) discusses the trends and problems in the field of digital evidence before the United States Courts of Appeals and records the history of how judges have approached the issue of digital evidence, showing that many unresolved issues remain in ways courts use to determine the scientific reliability of digital forensic measures. One of the most urgent issues that are posed by Horsman (2019) is the following one: the admissibility of automated forensic tools, i.e. programme software that processes digital evidence without human intervention in every step of its analysis, casts doubt on the reliability and transparency that current admissibility standards are ill adapted to handle. The issues of admissibility in civil law systems have a different approach. According to Dmitrieva and Pastukhov (2023), the official list of evidence accepted in criminal procedure codes of civil law was not intended to accommodate unique features of digital data. The digital records in France, Germany, or the Netherlands, and other countries, do not have to be incorporated into specific types of evidence, as they do, by judicial interpretation, but they generate inconsistent and unpredictable admissibility results.

Komalasari and Mustafa (2023) discuss how electronic evidence can enhance integrity in the justice system and believe that the efficiency of digital evidence in criminal trials cannot solely be explained by the technical quality of digital evidence, but also by the legal and institutional contexts under which such evidence should be used. By introducing a framework of the legal admissibility of digital evidence obtained with the open-source forensic tools, Ismail and Ariffin (2025) make an important contribution to the literature on admissibility in forensic tools as a more recent category of digital evidence whose admissibility is highly contentious in most jurisdictions due to the lack of commercial certification and peer-reviewing history of commercial forensic software. In Goodison *et al.* (2015), a thorough evaluation of the state-practice of digital evidence in the criminal justice system of the United States is presented, which documented the practical challenges of working with digital evidence on a large scale by law enforcement, prosecutors, and courts.

Chain of Custody and Forensic Integrity

The procedural mechanism through which the integrity of physical evidence is guaranteed in criminal proceedings is the chain of custody - the ongoing, documented process of who handled the evidence, when and what was done to it. The way it applies to digital evidence has unique issues that are brought about by the ease of manipulation of digital evidence, the technical complexity of forensic activity being conducted on digital evidence, and the decentralization of the digital evidence collection process by networks and jurisdictions. Arshad *et al.* (2018) offer an in-depth overview of scientific validation concerns that surrounds digital evidence and chain of custody integrity is one of the underlying challenges that govern admission of digital evidence in a criminal trial. Miller (2022) records the pragmatic outlooks of prosecutors and investigators on digital evidence issues, where chain of custody management is noted as the ongoing operational challenge especially in the large-volume investigations where evidence can be handled by several hands and through numerous forensic processes before trial.

Reinventing the chain of custody issue with the utilization of the blockchain technology has received significant academic interest as a possible resolution to the issue of integrity of the digital evidence. Tsai *et al.* (2021) consider how the distributed ledger technology could be applied to the custody of evidence during the criminal investigation process because the immutability and transparency characteristics of blockchain can offer a more robust and resistance to tampering audit trail than the traditional paper-based custody records. Batista *et al.* (2023) present a systematic literature review of the blockchain application in the area of chain of custody in physical and digital evidence that offers considerable opportunities but faces implementation issues connected to the scale, court admissibility of blockchain entries, and barriers to adoption by institutions. Further development of this literature is done by Park and Jeong (2026), who offer a blockchain-based digital evidence management system that unites the forensic processes with the multi-party authorisation processes which could be seen as a technical model of governance that is based on the forensic science as well as the legal framework. The standard digital forensic process model, as shown in Figure 1 below regulates evidence manipulation in criminal cases.

DIGITAL FORENSIC PROCESS MODEL FOR CRIMINAL PROCEEDINGS		
01	IDENTIFICATION	Identification and reporting of possible digital evidence sources at the scene or in digital systems; identification of evidentiary relevance and legal jurisdiction to be collected (Casey, 2011; Sabillon et al., 2017).
↓		
02	PRESERVATION	The protection of digital evidence against corruption, alteration, or deletion; use of write-blockers; forensic imaging of storage media; the creation of cryptographic hash values to create a baseline integrity (Arshad et al., 2018; Pollitt, 2013).
↓		
03	COLLECTION	Legal seizure of digital equipment and information with the relevant legal authority; the description of collection practices; the preservation of an intact chain of custody since the time of seizure (Miller, 2022; Goodison et al., 2015).
↓		
04	EXAMINATION	Analysis of the collected digital evidence with the help of approved forensic tools and procedures; file recovery; metadata recovery; decryption with authorisation (where appropriate) (Garfinkel, 2010; Horsman, 2019
↓		
05	ANALYSIS	The analysis of investigated data in the framework of the criminal investigation; the correlation of digital evidence with other evidence; the creation of the expert opinion about the importance of the digital findings (Nance et al., 2012; Ismail and Ariffin, 2025).
↓		
06	PRESENTATION	Delivery of digital evidence results to legal participants, including prosecutors, defence counsel, and courts, in a way that makes sense; expert testimony; disclosure (Mason and Seng, 2021; Novak, 2020).
↓		
07	CHAIN OF CUSTODY VERIFICATION	Ongoing records and validation of the integrity of digital evidence that it has been preserved during all the previous steps; blockchain-based or cryptographic audit trails that offer tamper evidence of records (Tsai et al., 2021; Park and Jeong, 2026; Batista et al., 2023).

Figure 1: Digital forensic process model for criminal proceedings

Source: Constructed from Casey (2011); Sabillon et al. (2017); Arshad et al. (2018); Pollitt (2013); Miller (2022); Goodison et al. (2015); Garfinkel (2010); Horsman (2019); Nance et al. (2012); Ismail and Ariffin (2025); Mason and Seng (2021); Novak (2020); Tsai et al. (2021); Park and Jeong (2026); Batista et al. (2023).

Problems of Cross-Border Digital Evidence

The distributed nature of the global internet architecture and the popularity of cloud computing has resulted in a scenario where digital evidence that can be used in a criminal process in one jurisdiction is regularly stored on servers in another, on which the service providers incorporated in a third country manage data protection policies which can contradict the criminal process policy of all three. The recent analysis of the cross-border criminal investigation and digital evidence offered by Casino *et al.* (2022) is the most detailed, presenting the legal, technical, and institutional obstacles that complicate the mutual legal assistance in the cases of digital evidence and show the insufficiency of the current international cooperation systems. The Mutual Legal Assistance Treaty (MLAT) system, which was exercised to operate in the era of tangible evidence and paper bookkeeping, is generally recognized as being too slow and unwieldy to satisfy the practical requirements of the transnational digital evidence collection (Ruan *et al.,* 2013).

Ruan *et al.* (2013) and Quick and Choo (2014) look directly at the particular issues of cloud forensics, which they see as the multi-tenancy structure of cloud infrastructure, the dynamically allocated storage resource and the jurisdictional uncertainty of cloud data as particular challenges that the traditional forensic practices, and the legal system, cannot handle. The analysis is furthered by Losavio *et al.* (2016) into the context of the IoT, where big amounts of personal and behavioural information are generated by networked instruments and must be encompassed by definitive legal structures that establish the rights of law enforcement to such information. In a pioneering prospective study, Garfinkel (2010) was able to indicate the research agenda the coming decade of digital forensics would have to catch-up on - a programme that, fifteen years later, has only been partially achieved, a serviceable indicator of the lag in structure between technological change and forensic and legal change. The rise of AI-generated evidence as a new category adds to these cross-border challenges: AI systems fed on the data of various jurisdictions and used across the borders generate chains of accountability that the current frameworks of mutual legal assistance are completely unprepared to handle.

MATERIALS AND METHODS

The research methodology used in this article is theoretical and conceptual which is in line with the purpose of the paper to develop a normative governance model on digital evidence use in criminal cases instead of producing or examining empirical data. Theoretical and conceptual scholarship takes a secure and appreciated place in the field of both legal scholarship and digital forensics research and serves to extrapolate existing knowledge, pinpoint analytical gaps, and develop new frameworks, which are able to inform further empirical research and reform of the law in institutions (Pollitt, 2013; Garfinkel, 2010; Stoykova, 2024).

The approach of methodology is based on the three main traditions of thought. To start with, the theory of evidence law that includes the doctrinal study of admissibility rules, the theoretical basis of the chain of custody rule, and the normative basis of the fairness and reliability requirements regarding criminal evidence gives the legal analytical context in which the digital evidence issues are framed (Leroux, 2004; Mason and Seng, 2021; Novak, 2020). Second, the scientific basis of assessing the legal frameworks under consideration is furnished by the digital forensics scholarship such as the technical literature on the model of forensic processes, tool validation, and mechanisms of evidence integrity (Casey, 2011; Arshad *et al.,* 2018; Sabillon *et al.,* 2017; Nance *et al.,* 2012). Third, the theory of governance, which includes the literature on the regulatory design, institutional structures, and governance of emerging technologies, would offer the analytical tools to assess the sufficientness of the existing frameworks and develop the proposed governance model (Stoykova, 2024; Komalasari and Mustafa, 2023).

The study entailed a scientific review of scholarly publication on the topic of digital evidence utilization in criminal cases, policy reports and legal tools. Searches in Scopus, Web of science, Hein Online, Google Scholar and the Social Science Research Network were used to identify literature. Such terms as: digital evidence criminal proceedings, digital forensics admissibility, chain of custody digital evidence, cloud forensics jurisdiction, blockchain evidence integrity, and procedural fairness digital evidence were used as search terms. The search was limited to the publications of 2004-2026, with the focus on the works published after 2010 that represent the latest stages of the technological and legal evolution. A preliminary list of about eighty sources was formed; after applying the inclusion criteria, i.e. the relevance to the legal and forensic governance setting, theoretical importance, and the quality of scholarly work, twenty-five sources were included in the systematic examination. These criteria of selection filtered out solely technical forensic literature that did not have a legal or governance aspect, and empirical research on particular jurisdictional practice that did not have conceptual generalizability, lest the synthesis of conceptualizations be disrupted. The instigated conceptual framework is the one that was promoted in the Results and Discussion section using the three theoretical lenses applied to the identified regulatory challenges in the Literature Review section that provided a synthesis of normative nature and is the main scholarly contribution of the article. Being a conceptual paper, the article does not test hypotheses, produce primary data, and make empirical assertions about the real practice of any jurisdiction. It has made its contribution in the form of construction and justification of theoretically based governance framework that can influence future empirical research, legislative change, and institutional design in a variety of legal systems at the same time. The four-pillar structure is based on the multi-dimensional nature of the regulation problem and the necessity of a structure that would be accommodating to the divergent procedural culture of common law and civil law jurisdictions - a requirement that single-dimensional regulatory proposals have never succeeded in fulfilling.

RESULTS AND DISCUSSION

The theoretical discussion leads to two main finds, which are reported and debated in syntactic form, one, an organised comparative study of admissibility criteria used in the context of digital evidence, and, second, a suggested conceptual structure of governance based on four mutually supporting normative pillars, which are intended to mitigate the structural failures found in the literature review. The sub-sections discuss the implications of these findings to the criminal procedure law, the practice of the digital forensics and the institutional design of criminal justice systems.

Comparative Analysis of Admissibility Criterion

As it is found in the literature review, in all the different criminal procedures reviewed in the academic record, the six dimensions have always been the same as the normative underpinnings of the admissibility of digital evidence authenticity, reliability, integrity, relevance, proportionality and fairness, and chain of custody. These criteria have different normative roles and are operationalised by different verification processes, but are not analytically independent - each of them assumes and supports the other, and their governance must be handled in accordance with their presence and interdependence as a system not as individual demands. Leroux (2004) fixes the authenticity and integrity as the threshold criteria, without which no further normative evaluation can be done. Horsman (2019) shows that the reliability criterion presents acute challenges to the admissibility of automated forensic tools, whose inner workings could be obscured to the legal actors who have to review the results obtained by these tools - a problem that becomes even more critical as AI-assisted forensic analysis becomes more widespread. Stoykova (2021) claims proportionality and fairness as formally acknowledged in most criminal procedure systems, but systematically not being applied in the digital evidence context, creates unchecked risks to the assumption of innocence as the fact-finders give computer-generated outputs undue epistemic power. According to Stoykova (2024), one of the governance mechanisms that are specifically aimed at mitigating these fairness shortcomings is a new right to procedural accuracy - which the current structure implements and operationalises as one of its fourth pillars. The comparison of these criteria and their main verification mechanisms in terms of their specifics is given in Table 2 below.

Table 2: Comparative analysis of digital evidence admissibility criteria in criminal proceedings

Admissibility Criterion	Legal Standard	Verification Mechanism	Scholarly and Judicial Significance
Authenticity	The digital evidence has to be what it claims to be and it should not have been manipulated since its collection	(MD5/ SHA-256) hash value checking; digital signature; forensic photography of original media using write-blockers	The threshold test of admissibility in all significant major common law and civil law jurisdictions is authenticity (Leroux, 2004; Casey, 2011).
Reliability	The digital evidence collection, preservation and analysis processes and tools should be scientifically valid and reproducible	Certified forensic instruments; compliance with the ACPO, NIST, or ISO regulations; peer checking of the forensic methodology	According to Horsman (2019), one of the structural barriers to admissibility is judicial lack of familiarity with the reliability of automated forensic tools.
Integrity	Evidential content must be shown to be complete and unaltered throughout the chain of custody from collection to courtroom	Unbroken chain of custody documentation; cryptographic hashing at each transfer point; blockchain-based custody records	Integrity failures render evidence inadmissible and may constitute grounds for exclusion of related evidence (Batista *et al.,* 2023; Stoykova, 2021)
Relevance	Digital evidence should be probative in nature- it should increase or decrease the likelihood of a fact in issue without it	The court analysis of the nexus between digital evidence and the crimes committed, the expert testimony of the importance of data	The trial court determines relevant, which is a condition precedent to admissibility in any of the principal criminal procedure systems (Novak, 2020; Mason and Seng, 2021).

Equal Treatment and Fairness.	The prejudice, confusion, as well as unfairness to the accused, should not outweigh the probative value of the digital evidence substantially	The assessments of the judicial balancing; exclusionary rules; the right to challenge digital evidence by expert counter-analysis.	Stoykova (2021) also singles out the undiscussed systemic risks to fairness that digital evidence creates due to the cognitive authority of the fact-finders
Chain of Custody	A chronological, recorded history of the individuals that touched the digital evidence, when, and what actions were done at each step.	Modern custody records; tamper-evident packages; electronic audit logs, system of multi-parties authorisation.	The most widespread methods of undermining the admissibility of digital evidence in practice include chain of custody failures (Miller, 2022; Park and Jeong, 2026).

Source: Synthesised from Leroux (2004); Casey (2011); Horsman (2019); Novak (2020); Stoykova (2021); Mason and Seng (2021); Batista et al. (2023); Miller (2022); Park and Jeong (2026); Stoykova (2024); Dmitrieva and Pastukhov (2023).

The biggest loophole that has been revealed through the comparative analysis is the admissibility of the results of automated forensic tools. As Horsman (2019) shows, the judicial process of assessing the reliability of a tool needs some degree of technical expertise that most legal participants lack, and the lack of certification systems makes courts regularly tasked with reviewing evidence created by a tool whose scientific soundness has not been thoroughly tested. It is proposed that the suggested framework would fill this gap by introducing the forensic integrity pillar into the framework and making the forensic tools required to be certified and using validated methods as a condition of admissibility to place digital forensics on an equal footing with other types of scientific evidence in a criminal trial.

Suggested Governance Framework of Digital Evidence

The article is based on the admissibility analysis and the detection of structural gaps in current frameworks, as well as introduces a proposed governance framework of digital evidence in criminal proceedings. It is structured as a set of four normative pillars that are mutually interdependent and address the different aspects of the regulatory issue, and underpinned by two implementation mechanisms that are international harmonisation and technological adaptation.

The first pillar, which is the legal standards, provides the necessity of consistent, technology-neutral, and periodically updated statutory provisions on the admissibility, collection, and use of digital evidence in a criminal case. The normative underpinnings of this pillar are presented by Stoykova (2024) and Mason and Seng (2021), who hold that the ad hoc development of the law of digital evidence imposed on the judiciary to decide case-by-case is not enough to bring the needed systemic clarity and consistency needed by the criminal justice actors. The key institutional figure that will enforce this pillar is the legislature, acting on specific digital evidence laws that outline legal power to collect such evidence, minimum admissibility requirements, as well as mandate to disclose such evidence to the defence. The lightest standard is the technology-neutral statutory framework, which must be regularly reviewed (at least once every five years), in order to accommodate technological change, without necessarily necessitating that the legislation be redrafted to reflect each new category of evidence.

The second pillar is forensic integrity which deals with scientific validity of methods and tools employed in gathering, preservation and analysis of digital evidence. According to Arshad *et al.* (2018), resource gaps that include the lack of the compulsory certification of the tools and uneven enforcement of the forensic standards are associated with structural threats to the scientific reliability of the digital evidence. Ismail and Ariffin (2025) are a step in the right direction by developing a given framework of the legal acceptance of evidence obtained by using open-source forensic tools. The implementing institution is a free-standing body of forensic accreditation - similar to bodies that regulate DNA forensics - and which has the authority to certify tools, audit laboratories, and issue methodology standards that can be applied as guides of admissibility in courts.

The third pillar chain of custody deals with integrity of the record of evidence between collection and courtroom. The combined efforts of Batista *et al.* (2023), Tsai *et al.* (2021), and Park and Jeong (2026) confirm blockchain based chain of custody as the most promising that is currently available to provide tamper-evident, multi-party-verified records of custody. The implementing actors include law enforcement agencies, forensic laboratories and offices of prosecutors all of which need to be involved in a common digital custody infrastructure that can generate court-admissible audit trails. Fairness and rights is the fourth pillar, which touches on the basic duty of criminal justice system to guard accused persons against wrongful conviction. According to Stoykova (2021) and Dmitrieva and Pastukhov (2023), the normative underpinnings are based on the idea that the safeguarding of the presumption of innocence and the right to a fair trial should be placed as normative active regulation demands and not as principles of residuation. The implementation vehicle is a structure of procedural rights that are mandatory in nature such as the rights to independent forensic analysis of digital data, the right to the disclosure of the procedures, as well as the right to a reasonable decision by a judge related to the reliability of digital evidence, and is enforceable through defence counsel and subject to review on appeal. The proposed governance structure and institutional structure are demonstrated in Figure 2 below.

The chain of custody aspect of the discussion shows

PROPOSED GOVERNANCE FRAMEWORK FOR DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS	
CO-REGULATORY ARCHITECTURE: Statutory authority combined with professional forensic standards and judicial oversight	
PILLAR I LEGAL STANDARDS	Equal guidelines of admissibility across the borders; rules of statutory digital evidence to establish who is allowed to collect the evidence; judicial practice training programmes; cross-jurisdictional legal instruments and cross-border mutual recognition. Reference: Stoykova (2024); Mason and Seng (2021).
PILLAR II FORENSIC INTEGRITY	Mandatory certification of forensic tools by accredited bodies (ACPO, NIST, ISO); standardised examination methodologies; independent audit mechanisms for forensic laboratories; scientific peer review of novel forensic processes. Source: Arshad et al. (2018); Ismail and Ariffin (2025).
PILLAR III CHAIN OF CUSTODY	Custody records designed on blockchain which have tamper-evident and continuously verifiable audit trails; multi-party authorisation of evidence transfer; cryptographic verification of all transfer points; paper-based custody records are substituted with digital custody records. The reference list is omitted. . Source: Park and Jeong (2026); Batista et al. (2023); Tsai et al. (2021).
PILLAR IV FAIRNESS AND RIGHTS	Protection by way of presumption of innocence, that is, built in as an affirmative regulatory requirement; the accessibility of digital evidence analysis by defence that is conducted independently; the right to challenge AI-generated and automated forensic results; procedural accuracy as a justiciable right. Due to different sources, we refer to Stoykova (2021); Dmitrieva and Pastukhov (2023).
ALL FOUR PILLARS ARE INTERDEPENDENT AND MUTUALLY REINFORCING	
INTERNATIONAL HARMONISATION The cross-border joint legal assistance system; the international standards of digital evidence; the multilateral agreements on forensic cooperation to combat the problem of jurisdiction fragmentation (Casino et al., 2022; Komalasari and Mustafa, 2023).	TECHNOLOGICAL ADAPTATION Constant update of the frameworks to be used to accommodate new evidence types (IoT, AI-generated data, blockchain); investment in forensic research capacity; judicial and prosecutorial technology expertise (Garfinkel, 2010; Losavio et al., 2016).

Figure 2: Proposed governance framework for digital evidence in criminal proceedings
Source: Constructed from Stoykova (2024); Mason and Seng (2021); Arshad et al. (2018); Ismail and Ariffin (2025); Park and Jeong (2026); Batista et al. (2023); Tsai et al. (2021); Stoykova (2021); Dmitrieva and Pastukhov (2023); Casino et al. (2022); Komalasari and Mustafa (2023); Garfinkel (2010); Losavio et al. (2016).

the sharpest concern of the practical problem of digital evidence regulation and the most promising technological tool. Miller (2022) reports on the widespread practical challenges of records of sufficient chain of custody in digital evidence in cases of high-volume criminal investigations and Batista *et al.* (2023) and Park and Jeong (2026) prove the technical viability of blockchain-based custody systems that can provide continuously verifiable, tamper-evident audit trails. Theoretical contribution of the article is placing blockchain-based chain of custody into a wider governance context that does not focus on the technical aspect of custody integrity only but on the legal admissibility of blockchain records as evidence of custody a question, Tsai *et al.* (2021) find that the legal standards pillar is meant to answer.

The most structurally complicated issue and the one that can be hardly addressed using domestic reform is the cross-border aspect of digital evidence governance. As demonstrated by Casino *et al.* (2022), the lack of international litigation also hampers the successful criminal prosecution of offences targeting the global structure of the internet because of the fragmentation of the international legal framework based on conflicting national admissibility standards, contradictory data protection regimes, and poor law-enforcement mechanisms. The international harmonisation mechanism ensured by the framework envisions the creation of binding international instruments with specific focus on digital evidence, i.e. instruments that extend to cover cloud forensics, the IoT evidence, and blockchain records and which introduce mutual recognition requirements on digital forensic certifications between signatory states.

The fairness and rights aspect reverts to the underlying normative issue on which the whole analysis is animated. According to Stoykova (2021), the cognitive power that the digital evidence has on the fact-finders, namely the judges and juries who are likely to perceive computer-generated outputs as self-affirming, is a structural threat to the presumption of innocence. The fairness and rights pillar of the framework reacts by instilling positive procedural requirements such as right to challenge digital evidence by independent expert examination, right to forensic technique disclosure, and right to judicial appraisal of credibility of digital evidence in a rational manner as a matter of governance and not as an idealistic principle. This is put in the context of a fresh right to procedural accuracy, which this article uses as the normative background of the fourth pillar and which is projected to an explicit governance duty on criminal justice institutions.

A major conflict of the given framework deserves to be mentioned explicitly: the conflicting interests of the investigative effectiveness and the protection of the rights of the individuals. The law enforcement practices need to be timely and comprehensive access to digital evidence to effectively investigate the serious crime; criminal suspects and defendants need to enjoy strong procedural protections against the erroneous admission of unreliable or disproportionately intrusive digital evidence. The article by Goodison *et al.* (2015) records the practical strain on the police that the sheer amount and multifaceted nature of digital evidence present in the contemporary investigation; the article by Nance *et al.* (2012) describes the disconnect between the laboratory forensic practice and the realities of work in the field. This tension is resolved in the proposed framework by a degree of proportionality, i.e. matching the strength of forensic standards and admissibility requirements to the severity of the crime and the centrality of digital evidence to the case against the offender, as opposed to the uniformity offered by uniform requirements that operational implementation may in practice be impossible in lower-stakes investigations. Komalasari and Mustafa (2023) propose a more complementary analysis because the effectiveness of investigations and the protection of individual rights, under the proper governance structure, are complementary.

The mass digital surveillance aspect of the structure is another aspect that should be highlighted as the present challenge, especially with the increasing involvement of intelligence-based digital evidence in criminal courts with the help of derogations to standard admissibility norms. The rights implication of using bulk interception data, facial recognition results, and location data collected by telecommunications providers as evidence during criminal trials are the rights of presumption of innocence, the right to remain silent, and the fairness and rights pillar of the framework must be viewed as ensuring that the fairness component of this pillar is met. It is a lowest requirement of a governance framework that is adequate to the modern digital evidence environment to ensure that evidence obtained through mass surveillance is as admissible, must be disclosed, and is entitled to defence challenge rights as evidence obtained in digital form that has not been obtained through mass surveillance.

CONCLUSION

This article offers theoretical and conceptual insight into the use of digital evidence in criminal proceedings by proposing a governance model built on four normative pillars: legal standards, forensic integrity, chain of custody, and fairness and rights, supported by international harmonisation and technological adaptation. The analysis shows that existing legal regimes are often inadequate for the challenges posed by volatile, distributed, and technologically complex forms of digital evidence. This difficulty is intensified by the rapid emergence of new evidentiary sources such as cloud computing, Internet of Things devices, artificial intelligence, and blockchain systems.

The article makes three main contributions. First, it provides a systematic account of the nature, attributes, and evidentiary concerns of digital evidence. Second, it supports comparative understanding of admissibility principles across jurisdictions while identifying key normative and operational gaps. Third, it advances a four-pillar governance framework that integrates legal, forensic, technological, and rights-based values into a unified model for reform.

Future research should develop stronger frameworks for international harmonisation, proportionality in admissibility decisions, and the regulation of AI-generated or AI-analysed evidence. Ultimately, digital evidence must be governed by frameworks that are technically informed, normatively sound, and institutionally robust to preserve the rule of law.

REFERENCES

Angel, O. E. M., Mercedes, C., Elisa, Q. L., & Gissel, M. R. M. (2024). Digital evidence as a means of proof in criminal proceedings. *Revista de Gestão Social e Ambiental, 18*(1), e04585. https://doi.org/10.24857/rgsa.v18n1-061

Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems, 14*(4), 956–976. https://doi.org/10.3745/JIPS.04.0084

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., & Endler, M. (2023). Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *Journal of Risk and Financial Management, 16*(8), Article 360. https://doi.org/10.3390/jrfm16080360

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. *Academic Press*. https://doi.org/10.1016/C2009-0-19445-5

Casino, F., Dasaklis, T. K., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of electronic evidence in criminal legal procedure. *Journal of Digital Technologies and Law, 1*(1), 155–178. https://doi.org/10.21202/2782-5108.2023.1.155-178

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7,* S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system. *RAND Corporation.* https://doi.org/10.7249/RR890

Horsman, G. (2019). Digital evidence: A review of the admissibility of the automated forensic tool. *Forensic Science International: Digital Investigation, 29,* 36–45. https://doi.org/10.1016/j.fsidi.2019.03.004

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*(1), e0331683. https://doi.org/10.1371/journal.pone.0331683

Komalasari, R., & Mustafa, C. (2023). Electronic evidence in the healthy justice system. *Jurnal Hukum dan Peradilan, 12*(3), 547–566. https://doi.org/10.25216/jhp.12.3.2023.547-566

Kumar, S., & Kumar, S. (2024). Reimagining the legislative framework: A historical analysis of decolonization and public voice in India's law-making. *American Journal of Society and Law, 3*(2), 16–30. https://doi.org/10.54536/ajsl.v3i2.3165

Leroux, O. (2004). Legal admissibility of electronic evidence. *International Review of Law, Computers & Technology, 18*(2), 193–220. https://doi.org/10.1080/1360086042000223508

Losavio, M., Pastukhov, P., & Polyakova, S. (2016). The Internet of Things and the smart city: Legal challenges with digital forensics, privacy, and security. *Security and Communication Networks, 9*(13), 2128–2137. https://doi.org/10.1002/sec.1469

Mason, S., & Seng, D. (Eds.). (2021). *Electronic evidence and electronic signatures.* University of London Press. https://doi.org/10.14296/221.9781911507260

Miller, C. M. (2022). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Digital Investigation, 42,* Article 301416. https://doi.org/10.1016/j.fsidi.2022.301416

Nance, K., Hay, B., & Bishop, M. (2012). Digital forensics: Beyond the laboratory. *IEEE Security & Privacy, 10*(6), 68–72. https://doi.org/10.1109/MSP.2012.148

Novak, M. (2020). Digital evidence in criminal cases before the U.S. Courts of Appeals: Trends and issues for digital forensics. *Journal of Digital Forensics, Security and Law, 14*(4), Article 3. https://doi.org/10.15394/jdfsl.2020.1603

Park, Y., & Jeong, D. (2026). A blockchain-based digital evidence management system: Integrating forensic procedures and multi-party authorization. *Information Processing & Management, 63*(1), 103946. https://doi.org/10.1016/j.ipm.2025.103946

Pollitt, M. M. (2013). The history of digital forensics. In *Advances in Digital Forensics IX* (pp. 3–15). https://doi.org/10.1007/978-3-642-41148-9_1

Quick, D., & Choo, K. K. R. (2014). Digital forensics out of the box: The use of enterprise search technologies to identify evidence on cloud storage. *Digital Investigation, 11*(2), 140–149. https://doi.org/10.1016/j.diin.2014.03.001

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics: An overview. In *Advances in Digital Forensics IX* (pp. 35–46). https://doi.org/10.1007/978-3-642-41148-9_3

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. J. (2017). Digital forensic analysis of cybercrimes: Best practices and methodologies. *International Journal of Computer Science and Information Security, 15*(7), 178–186. https://doi.org/10.2139/ssrn.3010363

Slom, F. A. A. (2024). The role of good governance in promoting human rights in Sudan. *American Journal of Arts and Human Science.* https://doi.org/10.54536/ajahs.v3i3.2884

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review, 42,* 105575. https://doi.org/10.1016/j.clsr.2021.105575

Stoykova, R. A. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review, 52,* 105912. https://doi.org/10.1016/j.clsr.2024.105912

Tsai, F. C., Chang, S. C., Lin, J. H., & Lin, C. H. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science, 187,* 218–223. https://doi.org/10.1016/j.procs.2021.04.054