Future Technology
Open Access Journal
ISSN 2832-0379

November 2026| Volume 05 | Issue 04 | Pages 284-298

Journal homepage: https://fupubco.com/futech

https://doi.org/10.55670/fpll.futech.5.4.23

Future Publishing LLC

Article

Cybercrime law and digital forensics: adapting legal frameworks for future technologies

Vishal Anand[1]*, Apoorva Singh[2], Anuj Kumar Singh[3], Dal Chandra[4], Rahul[5], Navpreet Singh[6], Krishna Kumar[7]

[1]Guru University Department of Law, Patna University, Patna, India
[2]Department of Law, Specialization in Criminal Law and Commercial Law, S.S Khanna Girls' Degree College, Prayagraj, India
[3]Institute of Legal Study & Research, GLA University, Mathura, India
[4]College of Law and Legal Studies Teerthanker Mahaveer University, Moradabad, India
[5]Department of FORENSIC, Specialization in Forensic Medicine, SGT University, Gurugram- 123029, Haryana, India
[6]Amity Law School, Amity University Punjab, India
[7]Department of Computer Science & Engineering, Specialisation in Computer Science & Engineering, Institute of Technology & Management, GIDA, Gorakhpur- 273001, Uttar Pradesh, India

ARTICLE INFO

Article history:
Received 02 April 2026
Received in revised form
07 September 2026
Accepted 21 September 2026

Keywords:
Cybercrime law, Digital forensics,
Electronic evidence, Forensic tool validation,
Technology-neutral regulation,
Legal admissibility

*Corresponding author
Email address:
vishalanand.law@gmail.com

DOI: 10.55670/fpll.futech.5.4.23

ABSTRACT

Linked authenticity, integrity, reliability, attribution, jurisdiction, and privacy challenges are created by digital evidence from cloud platforms, Internet of Things (IoT) devices, artificial intelligence (AI), large language models (LLMs), biometrics, drones, blockchain, and virtual environments. This review synthesizes scholarly and authoritative sources on cybercrime law, digital forensics, and emerging technologies through a structured narrative review. The review reveals a technical–legal divide: it emphasizes investigative efficiency, while acquisition, hashing, metadata, chain of custody, tool validation, and automated-analysis reliability require clarification for evidentiary scrutiny. Technology, evidence source, forensic challenge, legal risk, admissibility requirement, and governance response are linked through the Technology–Forensic–Legal Admissibility (TFLA) Framework. Primary artifacts are distinguished from analytical outputs; technical weaknesses are translated into legal consequences and safeguards. Standards and evidentiary rules are complemented; TFLA is conceptual, not empirically validated. Technology-neutral, technically informed, rights-compliant governance is supported through transparent documentation, corroboration, human oversight, and institutional competence. Digital-forensic system design is linked to trustworthy technology governance.

1. Introduction

1.1 Background and context

Crime and investigation have been transformed by digitalization. Cybercrime extends beyond unauthorized access, data theft, and network intrusion across cloud platforms, connected devices, encrypted communications, artificial intelligence, biometrics, drones, and virtual environments. Investigation, prosecution, and judicial decision-making are centered on digital evidence [1]. Forensic tools and investigative approaches are continually developed [2]. Digital evidence may be volatile, alterable, reproducible, and distributed across devices, providers, and jurisdictions. Logs, metadata, sensor records, communications, and analytical outputs must be handled with demonstrable authenticity, integrity, reliability, relevance, and continuity of custody [3]. Privacy, lawful access, procedural safeguards, and institutional responsibility are engaged [4]. Virtual-identity and asset evidence is created through metaverse activity [5]; analytical speed is improved through forensic automation, but explainability, validation, bias, and reproducibility are questioned [6]. Accuracy, consent, privacy, and bias concerns are introduced by biometric and multimedia evidence [7]; acquisition-legality and due-process questions are raised by leaked or hacked material [8]. Resilient investigative methods [9], dependable forensic procedures, institutional capacity, and judicial competence are complementary priorities [10].

1.2 Problem statement

Distributed and automated evidence may be underaddressed by rules for physical evidence or conventional computer records, with lawful access, ownership, jurisdiction, privacy, reliability, and admissibility uncertain. Investigative efficiency is often prioritized in technical scholarship, while acquisition workflows, hashing, metadata preservation, and tool validation may be underdeveloped in legal analysis. Integrated assessment of technological capability, forensic reliability, and rights-based safeguards is limited.

1.3 Aim and research questions

Adaptation of cybercrime law and digital-forensic practice to emerging technologies is examined through five research questions:

RQ1. How are cybercrime investigation and digital forensics affected by AI, cloud computing, IoT, LLMs, drones, biometrics, and virtual environments?

RQ2. What challenges do acquisition, preservation, hashing, metadata, chain of custody, tool validation, and automated analysis face?

RQ3. By what challenges are admissibility, authenticity, integrity, reliability, and judicial interpretation affected?

RQ4. How are privacy, accountability, due process, jurisdiction, and cross-border cooperation incorporated into digital-evidence governance?

RQ5. How can technologies, forensic challenges, legal risks, admissibility requirements, and governance safeguards be integrated?

1.4 Original contribution and structure

A critical interdisciplinary synthesis, operational forensic-control analysis, and Technology–Forensic–Legal Admissibility (TFLA) Framework are provided. Technology-specific forensic weaknesses are translated into legal risks, admissibility requirements, and safeguards; ISO/IEC, NIST, SWGDE, and evidentiary rules are not replaced. Methodology is explained (Section 2), literature synthesized (Section 3), legal governance, forensic processes, and emerging technologies examined (Sections 4–6), TFLA presented (Section 7), and research gaps, limitations, and conclusions addressed (Sections 8–10).

2. Review methodology

2.1 Review design and sources

Legal doctrine, forensic science, cybersecurity, ethics, and policy are integrated through structured narrative review. Literature identification, screening, quality appraisal, thematic classification, and comparative synthesis were used; no systematic-review claim or statistical meta-analysis is made. Sources were identified through Google Scholar, IEEE Xplore, ScienceDirect, SpringerLink, publisher and legal resources, and institutional collections. Standards, guidance, and legal instruments were supplied by ISO/IEC, National Institute of Standards and Technology (NIST), Scientific Working Group on Digital Evidence (SWGDE), Council of Europe, and European Union. Sixty sources were included: 33 scholarly publications and 27 technical, legal, regulatory, or institutional authorities.

2.2 Search strategy and publication period

Database-supported Boolean operators were used: "cybercrime law" AND "digital evidence"; "digital evidence" AND "admissibility"; "electronic evidence" AND "authenticity"; "digital evidence" AND "chain of custody"; "digital forensics" AND "cybercrime investigation"; "forensic tool validation"; "metadata analysis" AND "digital forensics"; "hashing" AND "digital evidence"; "cloud evidence" AND "jurisdiction"; "IoT evidence" AND "admissibility"; "AI forensic tools"; "explainable AI" AND "digital evidence"; "large language models" AND "digital forensics"; "LLM reliability" AND "forensic evidence"; "digital forensics" AND "privacy"; "cybercrime" AND "due process"; and "technology-neutral regulation".

Publications were mainly restricted to 2020–2025. Only foundational earlier sources were retained, including established forensic standards, legal instruments, technical guidance, and evidentiary principles.

2.3 Inclusion, exclusion, and screening process

Digital forensics, cybercrime law, evidentiary reliability or admissibility, emerging technologies, rights, cross-border cooperation, or governance were directly addressed by eligible sources. Journal articles, conference papers, scholarly chapters, substantive legal analyses, recognized standards, institutional guidance, legislation, and judicial authorities were considered. Research-question relevance, peer review or institutional authority, methodological or doctrinal transparency, technical/legal specificity, bibliographic completeness, and recency were appraised. A rigid citation-impact threshold was avoided given many 2024–2025 publications on rapidly developing technologies. Irrelevant or merely descriptive cybersecurity material, insufficient technical/legal depth, promotional or unsupported opinion, duplicates, unverifiable bibliography, and non-foundational out-of-window publications were excluded.

Six stages are reported (Table 1): identification, duplicate removal, title/abstract screening, full-text assessment, thematic classification, and synthesis. 180 records were identified: 150 academic-database records and 30 authoritative legal, technical, regulatory, or institutional records. Twenty-five duplicates were removed; 155 records were screened; 60 were excluded by title/abstract; 95 were assessed in full text. Thirty-five full texts were excluded: insufficient forensic–legal relevance (13), insufficient methodological/technical depth (8), promotional/opinion-based or incomplete bibliographic material (6), and non-foundational out-of-window publications (8). Sixty sources were retained: 33 scholarly publications and 27 authoritative sources. Screening is summarized in Figure 1.

2.4 Method of analysis

Sixty sources were thematically and comparatively organized into eight themes: cybercrime law; admissibility; applied forensic processes; emerging technologies; tool validation; privacy and ethics; cross-border evidence; and institutional/regulatory governance. Five dimensions were connected: technical handling and automation; legal/evidentiary requirements; procedural reliability, custody, and reproducibility; ethical and algorithmic governance; and institutional policy, competence, standards, and cooperation.

Table 1. Literature screening and selection process

Screening stage	Records (n)	Description
Stage 1: Identification	180	Records identified from academic databases (n = 150) and authoritative legal, technical, regulatory, and institutional sources (n = 30).
Stage 2: Duplicate removal	25 removed	Duplicate or repeated records were removed, leaving 155 records.
Stage 3: Title/ abstract screening	155 screened; 60 excluded	Records were screened for relevance to cybercrime law, digital forensics, electronic evidence, emerging technologies, forensic reliability, and admissibility.
Stage 4: Full text eligibility assessment	95 assessed; 35 excluded	Full texts were assessed using relevance, methodological/technical depth, legal relevance, publication quality, and bibliographic completeness.
Stage 5: Thematic classification	60 retained	Eligible sources were classified according to their principal legal, technical, forensic, ethical, policy, and governance contributions.
Stage 6: Final synthesis	60	Final evidence base comprised 33 academic/scholarly publications and 27 standards, legal, technical, regulatory, or institutional sources.

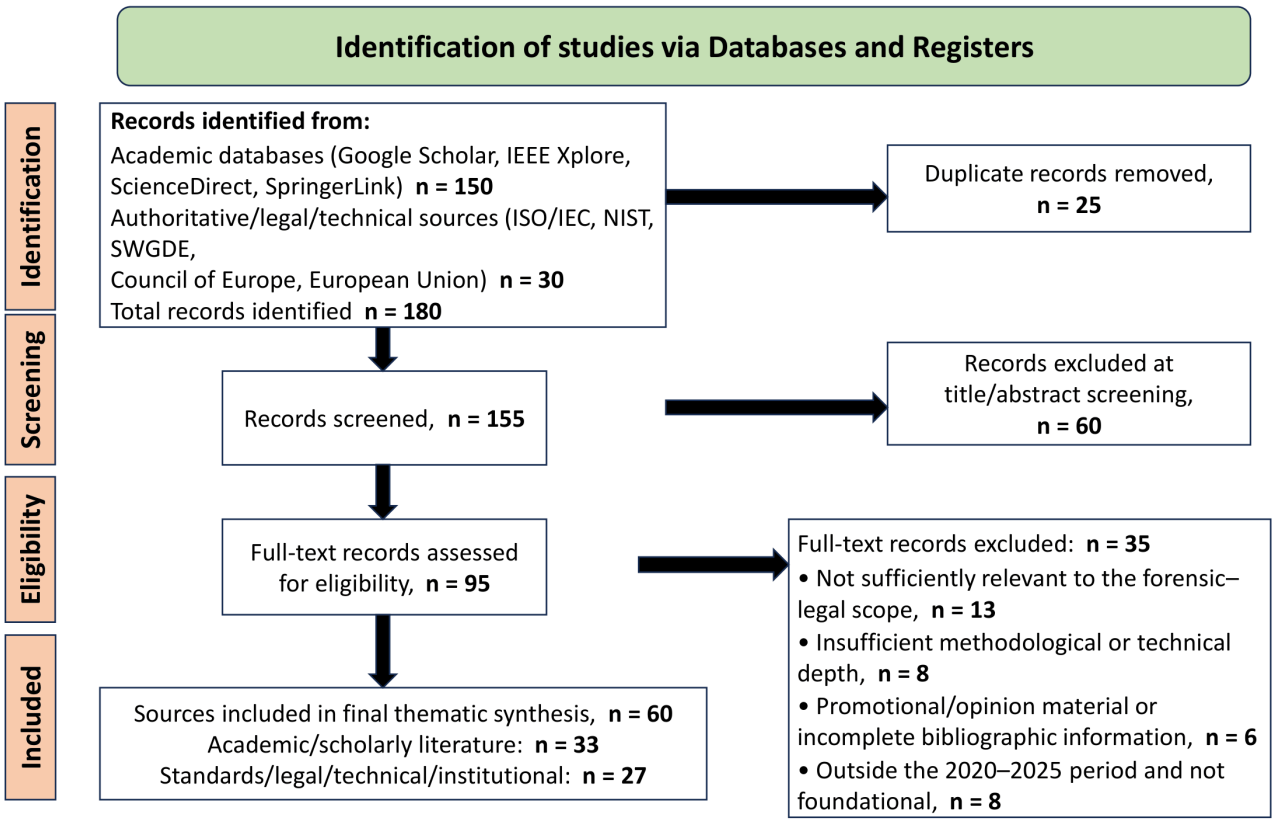

Figure 1. PRISMA-style flow diagram showing the identification, duplicate removal, title/abstract screening, full-text eligibility assessment, exclusion reasons, and final inclusion of sources in the structured narrative review

Automation versus explainability, rapid cross-border access versus rights safeguards, and technical integrity versus legal admissibility were compared. The integration gap informing TFLA was identified by comparing assumptions, strengths, limitations, and evidentiary implications. Independent duplicate coding was not performed; no inter-rater reliability coefficient was calculated. Reviewer subjectivity is acknowledged in Section 9.

3. Literature review and critical synthesis

Eight themes are linked through reliability, attribution, admissibility, and accountability questions created by changing evidence generation and analysis. Efficiency and scalability are emphasized in technical scholarship; procedural accuracy and contestability in legal scholarship [11,12]. Joint consideration is illustrated by drone research [13]; relationships are mapped. Technological evidence generation, forensic handling and validation, legal assessment, and rights-based governance are connected (Figure 2).

3.1 Main themes in literature

Technical reliability is linked with meaningful challenge [14]. Accuracy, privacy, consent, and attribution concerns are raised by biometrics and multimedia [15]; technical and legal coordination is required for transnational evidence [16,17]. Acquisition methods must be adapted for cloud, IoT, encrypted, and virtual environments [18]. AI-assisted analysis is expanding, but bias and transparency concerns remain [19]; anti-forensics must address deliberate concealment or manipulation [20]. Reliability is demonstrated through traceability, documentation, validation, and independent evaluation [21]. These requirements are complicated by provider-controlled cloud acquisition [22]; tool capability is distinguished from evidentiary credibility [23].

3.2 Governance, ethics, and comparative studies

Specialized cross-border production and preservation are examined in European research [24]; institutional adaptation to evolving cybercrime is emphasized broadly [25].

Automated and provider-generated evidence may be hard to challenge; reliability is linked to fairness and the presumption of innocence [26-28]. Privacy, sovereignty, proportionality, and human rights must be respected during faster access [27-30]. Reproducibility and verification are questioned for LLM analysis [31]; observable transactions and real-world attribution are distinguished in cryptocurrency investigations [32,33]. Scholarship is complemented by ISO/IEC forensic handling and investigative guidance [34-37], NIST and SWGDE operational guidance [38-41], and international cooperation and electronic-evidence instruments [42-44]. Among 33 scholarly publications, nine (27.3%) were primarily legal/evidentiary, seven (21.2%) technical/forensic, thirteen (39.4%) emerging-technology focused, and four (12.1%) ethical/governance focused. Twenty (60.6%) were classified as technical/forensic or emerging technology.

3.3 Comparative analysis of prior studies

Twelve thematically, methodologically, and technologically diverse studies are compared, not ranked (Table 2). Strong domain-specific contributions but limited integration of technology characteristics, forensic weaknesses, legal consequences, and safeguards are identified.

3.4 Agreements, disagreements, and research gaps

Traceable acquisition, validated analysis, preserved metadata and custody records, and independent scrutiny are consistently endorsed. Reliability is not established by digital origin alone. Four recurring tensions are identified: automation and efficiency [6] versus explainability and reproducibility [19,21,31]; rapid cross-border access versus rights safeguards [12,14,24,27,30,42–44]; technical integrity [34–41] versus lawful acquisition and procedural fairness [14,17,26]; and technological visibility versus reliable actor attribution [5,31–33]. An integration gap is identified: technological vulnerabilities are inconsistently translated into legal consequences and controls. The gap is addressed through six-layer TFLA (Section 7).

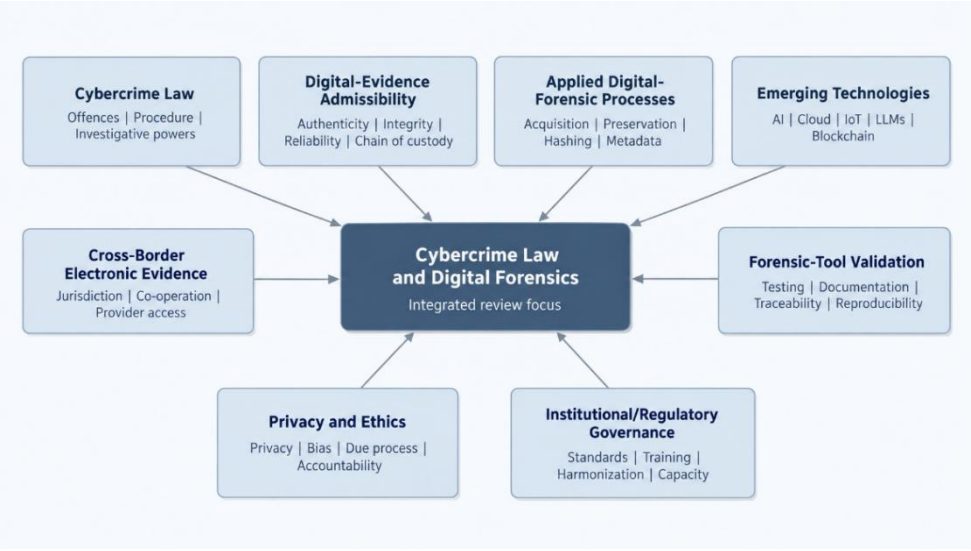

Figure 2. Thematic structure of the reviewed cybercrime law and digital forensics literature across eight interconnected analytical domains

Table 2. Comparative review of selected studies

Ref.	Domain / Study Type	Main Contribution	Key Finding	Main Limitation
[3]	IoT evidence; forensic–legal analysis	IoT handling is linked with admissibility	Courtroom use is complicated by volatile and distributed IoT artifacts	Technology/jurisdiction specific
[5]	Metaverse; framework study	A forensic structure for virtual environments is proposed	Adapted acquisition and preservation are required for virtual evidence	Limited legal-case application
[6]	AI/ML; technical review	AI/ML applications in digital forensics are reviewed	Scalability and analytical efficiency are improved through AI	Limited admissibility analysis
[12]	Digital-evidence governance; legal analysis	Procedural accuracy is linked with forensic reliability	Procedural risks are created by unreliable processing	Limited technical controls
[14]	Fair trial; legal analysis	Digital-evidence rules are connected with procedural fairness	A meaningful ability to challenge evidence is included in reliability	Limited technical validation
[16]	Cross-border evidence; forensic–legal analysis	Transnational evidence handling is examined	Technical and legal interoperability are both required	Jurisdictional barriers remain
[21]	Forensic reliability; assessment	Documentation, validation, and traceability are examined	Credibility is supported by demonstrable forensic procedures	Limited cross-jurisdictional scope
[22]	Cloud forensics; technical review	Cloud-forensic challenges are synthesized	Acquisition is complicated by provider control and dynamic storage	Limited legal integration
[24]	EU e-evidence; legal analysis	Specialized cross-border access mechanisms are examined	Electronic evidence is being moved toward dedicated procedures	EU-specific context
[31]	LLM forensics; case study	The reliability of LLM-assisted evidence is evaluated	Verification and expert oversight are required	Broader validation required
[32]	Cryptocurrency forensics; technical review	Tracing and attribution methods are reviewed	Multiple forensic techniques are required for attribution	Rapidly evolving tools
[33]	Blockchain investigation; forensic-system study	Forensically sound tracing is emphasized	Integrity and defensible procedures are required	Cryptocurrency-specific focus

4. Cybercrime law and digital evidence governance

Lawful acquisition, technically reliable handling, source authentication, integrity, and jurisdiction-specific admissibility must be established [21-23]. Requirements are complementary: cloud-export completeness or provenance cannot be established through lawful access, while an intact artifact may have been obtained unlawfully or disproportionately. Lawful access, acquisition, preservation, custody, validation, expert interpretation, and judicial assessment are linked (Figure 3). Reliability, evidentiary weight, or admissibility may be affected by stage-specific weaknesses.

4.1 Legal admissibility and procedural safeguards

Authenticity is assessed against claimed evidence identity; integrity against material alteration; reliability against method, tool, or interpretation. Possession, access, transfer, and examination are documented through chain of custody; these assessments are not replaced [17,21,23]. Sufficient authentication is required under U.S. Federal Rule of Evidence (FRE) 901; accurate processes or systems are addressed under Rule 901(b)(9). Specified electronic-process records and copied data may be certified under Rules 902(13) and 902(14). Hash comparison is recognized for unchanged-copy identification in the Rule 902(14) explanation [48]. Sufficient facts or data, reliable expert methodology, and reliable application are separately required under FRE 702; judicial scrutiny of reliability and conclusion scope is emphasized by the 2023 amendment [48]. Testability, peer review, error rates, methodological standards, and acceptance are identified under Daubert [49]. Frye was federally displaced, although general acceptance remains relevant and Frye-type approaches are retained in some state systems [50]. Attribution uncertainty is illustrated in United States v. Vayner: profile creation or control cannot be established solely through a name, photograph, and personal details [51]. Search should be authorized and proportionate, although unrelated third-party data may be captured. Acquisition procedures, tool versions and configurations, hashes, analytical steps, error characteristics, and limitations must be disclosed for meaningful challenge. Scrutiny may be restricted by opaque proprietary or AI methods [19,21,26].

4.2 Comparative legal approaches to digital evidence

India, the United States, England and Wales, and the European Union are compared (Table 3); statutory authentication, expert reliability, forensic quality, and cross-border access are distinguished. The predecessor Evidence Act is replaced by India's Bharatiya Sakshya Adhiniyam, 2023 (BSA), for proceedings governed thereby. Electronic-record certification is retained in Section 63; source and hash information is included in its Schedule [45]. The Information Technology Act's electronic-record and expert-examination provisions also apply.

Under the predecessor Evidence Act, the special procedure for secondary electronic records was emphasized in Anvar P.V. [46]. Certification requirements were reaffirmed in Arjun Panditrao Khotkar, with secondary output distinguished from original-device production [47]. U.S. FRE 901/902 authentication is separated from FRE 702/Daubert scrutiny of expert interpretation [48-50]. Under England and Wales' statutory Forensic Science Regulator Code, fit-for-purpose methods, validation, documented limitations, competence, technical records, configuration control, and revalidation after relevant changes are required [52]. Cross-border production and preservation mechanisms are governed by EU Regulation 2023/1543; no uniform national authentication test is provided [44]. Acquisition authority, forensic quality, and courtroom admissibility remain distinct governance layers.

Figure 3. Digital-evidence admissibility pathway linking lawful access, forensic acquisition, integrity preservation, chain of custody, tool validation, expert interpretation, and judicial assessment

4.3 Judicial interpretation and evidentiary precedents

In disputes, the relationship between artifact, source, production process, and alleged actor is often inadequately demonstrated. Electronic-record certification is connected with provenance and reliable production in Anvar P.V. and Arjun Panditrao Khotkar [46,47]. Webpage capture is distinguished from attribution to the alleged controller in Vayner [51]; expert-method validity and limitations must be scrutinized under Daubert [49]. Artifact authenticity, actor attribution, and analytical reliability are separated. These distinctions are applied to provider exports, AI scores, blockchain tracing, and LLM-supported conclusions: findings must be intelligible and contestable in court.

4.4 Jurisdiction, cloud evidence, and cross-border access

Territorial investigative powers are confronted by transnational offenders, providers, and data [16,24,27,30]. Cloud records may be replicated, dynamic, encrypted, or accessed only through provider interfaces [22]. Cooperation and electronic-evidence mechanisms are provided by the Budapest Convention [42], its Second Additional Protocol [43], and EU Regulation 2023/1543 [44]. Faster access must be evaluated against sovereignty, privacy, proportionality, and due process [24,27,30].

Legal authority, provider response, account/tenant, extraction method, timestamps, API/export logs, metadata, format, meaningful hashes, and limitations should be recorded. Provider selection or transformation should be documented separately from investigator-controlled acquisition. Access is legally authorized; provenance, completeness, and reliability of received evidence are established through forensic documentation.

4.5 Forensic tool validation and technology-neutral reform

Fitness for purpose is not demonstrated by forensic-tool popularity [23]. Reference data, repeatability, reproducibility, error characterization, version/configuration records, examiner competence, and independent verification are required [21,23,34-41]. Training-data, threshold, model-update, and opacity risks are added by AI and proprietary methods. Testability, limitations, error assessment, and reliable application are linked with evidentiary scrutiny under FRE 702/Daubert and UK regulation [48,49,52]. Stable lawful-authority, authenticity, reliability, proportionality, accountability, and contestability principles are applied through technology-neutral reform; compliance may be demonstrated through technology-specific procedures.

Table 3. Comparative legal and forensic approaches to digital evidence

Jurisdiction	Principal Framework	Primary Evidentiary Focus	Technical/Forensic Connection	Principal Challenge
India	Bharatiya Sakshya Adhiniyam, 2023; IT Act, 2000	Electronic-record admissibility, certification and authenticity	Device/source information, certification and integrity/hash documentation	Applying statutory requirements to cloud, distributed and emerging forms of evidence
United States	FRE 901, 902 and 702; *Daubert* jurisprudence	Authentication and reliability of expert evidence	Process/system accuracy, certification, hash identification, error-rate and methodology scrutiny	Authentication and explainability of complex or proprietary systems
England and Wales	Forensic Science Regulator Act/Code of Practice	Reliability and quality of forensic activity	Method validation, risk assessment, configuration control, competence and documentation	Maintaining validated practice as tools and software rapidly change
European Union	EU e-Evidence Regulation and national evidentiary rules	Cross-border production and preservation of electronic evidence	Provider records, preservation, provenance and transmission controls	Jurisdiction, fundamental rights, proportionality and cross-border harmonization

Those principles are translated through TFLA into evidence-specific risks and safeguards; platform-specific admissibility laws are not proposed.

4.6 Summary of legal and regulatory challenges

Legal and evidentiary concerns are linked with evidence contexts, technical controls, and governance responses (Table 4).

5. Applied digital forensic systems and electronic evidence

Identification, acquisition, preservation, examination, analysis, reporting, and presentation are linked across conventional and emerging digital-forensic systems [21-23]. Reliable conclusions must be traceably linked to sources, acquired representations, and analytical methods [34-41].

5.1 Digital evidence lifecycle and integrity controls

Relevant devices, accounts, platforms, and logs are identified. Acquisition-related alteration should be minimized; method, operator, time, source identifiers, tool/version, configuration, and limitations recorded. Imaging, logical extraction, memory capture, provider export, or API acquisition may be appropriate [22, 34, 38,39]. Secure storage, access controls, evidence identifiers, integrity checks, and custody records are required for preservation. Controlled copies are normally analyzed; transformations and derived artifacts distinguished from sources. Methods, findings, uncertainty, and limitations are reported [17,21,23]. Integrity, documentation, validation, and expert review are situated throughout forensic processing (Figure 4).

Figure 4. Applied digital evidence lifecycle showing integrity controls, documentation points, and admissibility safeguards across the forensic process

5.2 Hashing, metadata integrity, and anti-forensics

Integrity checking is supported by SHA-256 and SHA-3 [53,54]. Collision weaknesses in MD5 [55] and significant collision-resistance limitations in SHA-1 [56] are acknowledged. Legacy values may be retained for compatibility alongside a stronger contemporary hash. Bit-level consistency, not authorship, lawful acquisition, source accuracy, or completeness, is supported by matching hashes. Provenance and custody documentation are required. Exact hashed objects and acquisition stages must be recorded for potentially changing cloud/IoT evidence. Chronology and attribution are supported by timestamps, EXIF, geolocation, account/IP identifiers, and audit logs [23]. These may be altered through copying, synchronization, clock drift, processing, time-zone differences, or manipulation. Original values should be preserved, time references normalized as appropriate, and significant timestamps independently corroborated. Anti-forensics is characterized by timestomping, log wiping, metadata alteration, data hiding, and secure deletion [20]. Filesystem artifacts should be compared with application, network, server, cloud, journal, backup, and remote logs. Manipulation, not authorship, may be indicated by missing sequences or inconsistent timestamps; observation should be distinguished from inference.

5.3 Cloud and IoT evidence acquisition

Physical cloud-source control may be unavailable [22]. Legal authority, provider/service, account/tenant, scope, time range, API/export method, extraction time, returned metadata, format, hashes, and limitations should be documented. Provider filtering, aggregation, or transformation should be recorded; received packages hashed; responses and acquisition metadata retained. Package integrity must be distinguished from source provenance and completeness. IoT artifacts are distributed across devices, firmware, networks, companion applications, clouds, and connected services [3]. Identifiers, versions, account relationships, network/logging settings, and time configuration should be recorded; cross-system artifacts correlated. Volatile evidence should be prioritized, alteration minimized, and collection of unrelated personal information limited to lawful investigative scope.

5.4 Forensic tool validation and standards-based practice

Forensic methods must be validated for their intended purpose rather than assumed reliable because a tool is widely used [21,23,35,40,41,52]. Reference datasets or controlled cases with expected outcomes should be used; tool/build, plugins, parsers, configuration, environment, and updates recorded; repeatability tested under similar conditions; reproducibility through sufficiently documented independent confirmation. Parsing and timestamp errors, unsupported formats, and incomplete acquisition must be characterized. AI model/training-data, threshold, update, false-positive/negative, and explainability assessment are required [11,19]. Material automated findings must be source-verified or independently confirmed. Validation, competence, auditability, configuration control, and revalidation are connected through ISO/IEC guidance [34-37], NIST/SWGDE procedures [38-41], and regulator requirements [52].

5.5 Summary of applied forensic processes

Forensic processes, risks, evidentiary purposes, and controls are consolidated (Table 5).

Table 4. Legal, evidentiary, and technical controls in digital-evidence governance

Legal/Evidentiary Issue	Evidence Context	Recommended Technical Control	Court/Legal Concern	Governance Response
Authenticity	Cloud logs, IoT data, social media, communications	Provenance metadata, account/device identifiers, provider records	Whether evidence is what it is claimed to be	Certification and source documentation
Integrity	Files, forensic images, extracted datasets	Cryptographic hashing, secure storage, audit logs	Alteration or tampering	Standardized preservation procedures
Reliability	Forensic software, AI tools, automated analysis	Validation, reference datasets, error assessment, version/configuration logs	Reliability of method and conclusions	Expert review and independent verification
Attribution	Accounts, virtual identities, blockchain wallets	Cross-source correlation, device and network evidence	Connection between artifact and real-world actor	Corroboration requirements
Jurisdiction	Cross-border cloud/provider data	Provider records and acquisition documentation	Lawful authority and territorial competence	International cooperation mechanisms
Privacy	Device, cloud and IoT searches	Data minimization and scope controls	Overcollection and proportionality	Rights-based safeguards
Due process	Black-box and proprietary systems	Explainability, audit logging, disclosure of limitations	Ability to challenge evidence	Human review and adequate disclosure
Chain of custody	All digital evidence	Access/transfer logs, evidence identifiers and timestamps	Continuity and integrity	Standardized custody documentation
Institutional capacity	Complex forensic systems	Training, competency assessment, quality management	Inconsistent interpretation or practice	Specialist units and professional standards

Table 5. Applied digital forensic processes and legal relevance

Forensic Process	Primary Purpose	Main Technical Risk	Evidentiary Significance	Principal Control
Identification	Relevant evidence sources are located	Hidden, distributed, or provider-controlled data	Evidentiary scope and provenance are defined	Source and ecosystem mapping
Acquisition	Relevant data are collected or imaged	Volatility, encryption, alteration during collection	Authenticity and completeness are supported	Forensic imaging/API acquisition with complete acquisition logs
Cryptographic hashing	Bit-level integrity of a defined evidence object is verified	Weak algorithms or inappropriate hashing of dynamic evidence	Integrity is supported	SHA-256/SHA-2 or SHA-3 with recorded acquisition-stage hash values
Metadata analysis	Context is established and events are reconstructed	Clock drift, time-zone errors, legitimate metadata changes	Chronology and attribution are supported	Metadata preservation, normalization, and cross-source correlation
Anti-forensics assessment	Concealment or manipulation is identified	Timestomping, log wiping, data hiding, metadata alteration	Misleading reconstruction is prevented	Redundant artifacts, independent logs, backups, and inconsistency analysis
Chain of custody	Evidence handling is tracked	Incomplete transfer or access records	Continuity and integrity are supported	Standardized evidence identifiers and custody/access logs
Cloud acquisition	Remote/provider-controlled evidence is obtained	Dynamic data, provider transformation, distributed storage	Provenance and completeness are supported	Provider/API documentation, export metadata, immediate post-acquisition hashing
IoT acquisition	Distributed device/ecosystem evidence is recovered	Heterogeneous firmware, volatile data, clock inconsistency	Reconstruction and device attribution are supported	Device/firmware documentation and device–app–cloud correlation
Tool validation	Analytical reliability is established	Unknown errors, version/configuration dependence	Expert-method reliability is supported	Known-reference testing, version control, reproducibility, independent verification
Reporting	Findings and limitations are communicated	Overstatement or insufficient technical explanation	Judicial evaluation and contestability are supported	Transparent methods, limitations, uncertainty, and audit trail

Reliability is supported by mutually reinforcing controls, not isolated hashing, metadata, or tool output.

6. Emerging technology systems and forensic–legal risks

Emerging systems are differentiated by evidence provenance, volatility, interpretability, attribution, and long-term verification. Section 5 controls are complemented and TFLA informed by technology-specific risks.

6.1 AI, LLMs, and automated forensic analysis

Triage, malware classification, anomaly detection, multimedia analysis, and large-scale processing are supported [6,11]. Bias, opacity, false results, and version/configuration dependence must be addressed through documented inputs, preprocessing, models, thresholds, validation, limitations, and examiner verification [19,21]. LLM results may be affected by prompts, context, versions, instructions, and sampling; unsupported statements may be included [31]. Input evidence, prompt sequence, model/provider/version, configuration, and complete outputs should be preserved; material findings source-verified; important queries repeated for consistency assessment; contradictions or hallucinations recorded. A defensible workflow is:

Preserved Evidence → Prompt Record → Model/Version → Output → Consistency Check → Source Corroboration → Examiner Verification

LLMs are analytical aids; evidentiary reliance is placed on verified artifacts and examiner interpretation.

6.2 Cloud, IoT, and distributed evidence environments

Cloud authentication, account, audit, virtual-machine, API, and file-history records are provider-controlled and may be replicated, modified, or filtered [22]. Tenant/account, acquisition method, time range, metadata, transformations, and limitations should be evaluated. Jurisdiction, sovereignty, privacy, proportionality, and cross-border access requirements are not resolved by provenance controls [16,22,24,27,30]. IoT device, application, network, and cloud artifacts may be generated. Reconstruction is complicated by proprietary formats, firmware differences, weak logging, clock drift, and synchronization [3]. Human initiators are not identified through device activity. Device identifiers, authentication, application, network, and cloud records should be correlated; third-party privacy respected.

6.3 Drones, biometrics, multimedia, and virtual identity evidence

Activity, not necessarily operator identity, may be established through drone telemetry, GPS, controller, camera, device, and cloud/application records [13]. Attribution must be corroborated through accounts, controllers, devices, communications, and networks. Identity is not directly proven through biometric similarity. Reliability is affected by sample quality, algorithm/version, thresholds, false-match rates, demographic performance, spoofing resistance, and database composition [7,15]. Validated interpretation and corroboration are required for contested matches. Images, audio, and video may be edited, transcoded, enhanced, or synthetically generated. Prior authenticity cannot be established through post-acquisition hashes; metadata, encoding, source-device information, processing artifacts, and independent recordings should be inspected. Account/avatar activity, not necessarily human controllers, is identified through virtual-platform logs [5]. Accounts, authentication, IP/network records, devices, wallets, and communications should be correlated; platform and human attribution distinguished.

6.4 Blockchain forensics and attribution

Tracing is supported by blockchain transactions, addresses, transfers, and smart-contract interactions; real-world identity is not automatically disclosed [32,33]. Flows are traced through transaction graphs; control inferred through address clustering and UTXO common-input/change-address heuristics. Assumptions may be undermined by CoinJoin, collaborative transactions, wallet behavior, mixers, bridges, and obfuscation [32]. Observable transactions should be distinguished from heuristic inferences; corroboration obtained through lawfully obtained exchange/account records, IP data, wallet applications, keys, communications, financial records, or devices; tools, assumptions, confidence, and limitations documented [32,33].

6.5 Quantum risk and post-quantum evidence preservation

RSA and conventional elliptic-curve public-key signature/authentication schemes would be threatened by a sufficiently capable fault-tolerant quantum computer [57-60]. This threat is distinguished from risks to symmetric cryptography and hashes: SHA-256 evidence hashes are not automatically invalidated by potential signature vulnerability. Particular preservation planning is required for long-lived signatures, certificates, and trusted timestamps. ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) were finalized by NIST (2024) [57-59]. Through cryptographic agility, evidence-management mechanisms can be adapted while provenance and custody history are retained [60]. Algorithms, key types, certificates, signatures, and timestamps should be recorded; renewed timestamps, re-attestation, or migration documented for traceability of protected representations to original evidence.

6.6 Emerging technology maturity and forensic–legal risk

Relative maturity/adoption and forensic–legal risk are compared (Figure 5); opacity, volatility, provider dependence, attribution, reproducibility, cryptographic uncertainty, and available controls are considered. The map is illustrative, not an empirically calibrated risk score. Provenance vulnerabilities are retained in mature cloud/IoT systems; evidentiary verification or attribution is complicated by AI/LLMs and virtual platforms; longer-term authentication is threatened by quantum risks. These technology-specific evidentiary vulnerabilities and corresponding safeguards are consolidated in Table 6.

7. Proposed technology–forensic–legal admissibility framework

Technological characteristics, forensic reliability, legal risks, evidentiary requirements, and governance are connected through TFLA. Forensic standards [34-41] and legal rules [45-52] are complemented, not replaced.

Table 6. Technology–forensic–legal risk and validation matrix for emerging digital evidence

Technology	Principal Risk	Legal / Evidentiary Concern	Key Validation or Governance Control
AI forensic tools	Bias, false results, opacity, model drift	Reliability, explainability, due process	Model/version records, benchmark testing, error assessment, human verification
LLM analysis	Hallucination, non-determinism, prompt sensitivity	Reproducibility and contestability	Prompt/model logging, source corroboration, examiner verification
Cloud	Provider control, dynamic or transformed data	Authenticity, completeness, jurisdiction	Export/API records, metadata validation, provider documentation
IoT	Fragmented evidence, weak logs, clock drift	Attribution, authenticity, privacy	Device–app–network–cloud correlation and timestamp normalization
Drones	Operator uncertainty	Attribution and proportionality	Controller, account, device, and telemetry correlation
Biometrics	False matches, bias, sample quality	Identity reliability and privacy	Error/performance testing, version records, expert review
Multimedia	Editing or synthetic manipulation	Authenticity and provenance	Metadata/encoding analysis and source corroboration
Virtual platforms	Pseudonymous identity	Actor attribution and jurisdiction	Account–device–network–wallet correlation
Blockchain	Heuristic attribution and obfuscation	Real-world identity linkage	Graph analysis, documented heuristics, off-chain corroboration
Quantum/PQC	Future public-key obsolescence	Long-term authenticity	Crypto-agility, PQC migration, documented re-attestation

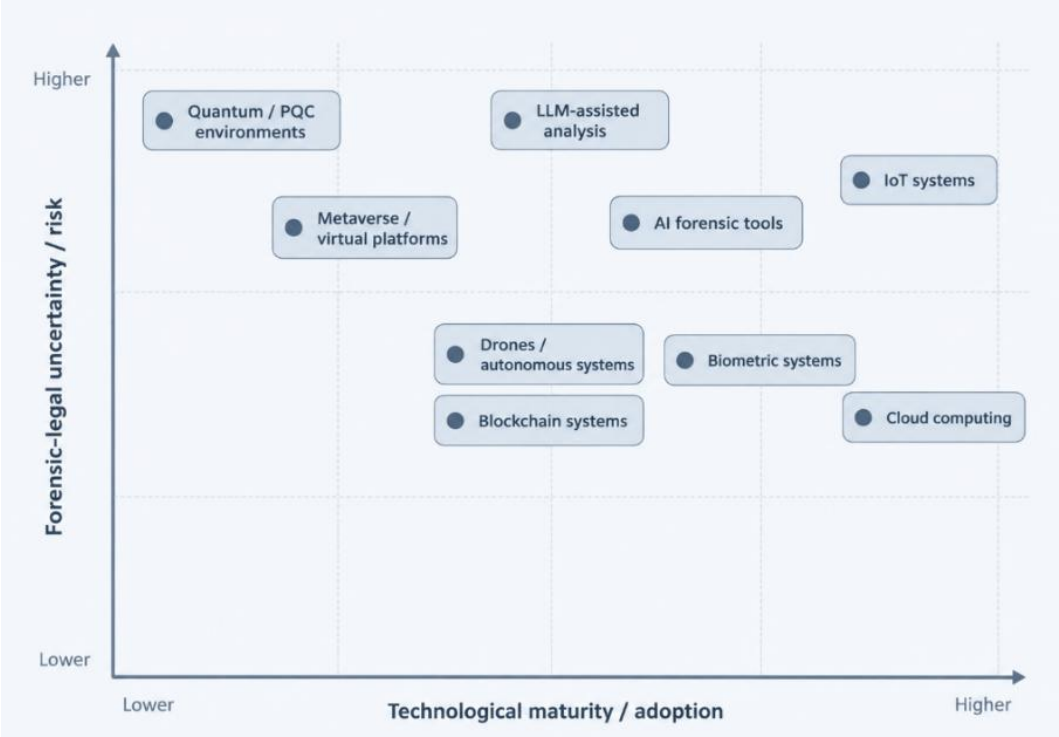

Figure 5. Qualitative map of emerging-technology maturity and forensic–legal risk based on technological adoption, evidentiary complexity, attribution difficulty, reproducibility, and maturity of forensic and legal controls.

Six linked layers are used for translation: technological weaknesses are identified, evidentiary consequences established, and appropriate safeguards selected:

Technology → Evidence Source → Forensic Challenge → Legal Risk → Admissibility Requirement → Governance Response

7.1 Rationale and six-layer architecture

Platform, provider, version, configuration, automation, and control environment are identified under Technology. Original files, logs, metadata, telemetry, communications, and transactions are distinguished from derived reports, classifications, scores, or summaries under Evidence Source. Source and analytical-tool reliability are considered separately. Volatility, incomplete acquisition, encryption, metadata/clock problems, provider transformation, opacity,

false results, or uncertain attribution are identified under Forensic Challenge. These weaknesses are translated into lawful-access, privacy, jurisdiction, reliability, or meaningful-challenge concerns under Legal Risk. Authenticity, integrity, relevance, reliability, attribution, material completeness, or procedural fairness are identified under Admissibility Requirement; validation, corroboration, metadata preservation, audit logs, certification, or oversight are specified under Governance Response. Layer assessments and outputs are summarized (Table 7). Analytically sequential TFLA may be iterated through further acquisition, validation, corroboration, or documentation to address unresolved weaknesses before reliance.

7.2 Relationship with existing standards and legal tests

Identification, acquisition, and preservation are addressed by ISO/IEC 27037; method suitability, analysis, interpretation, and investigation by ISO/IEC 27041–27043 [34-37]. Handling and validation are guided by NIST and SWGDE [38-41]. Authentication is addressed under FRE 901/902; expert reliability under FRE 702/Daubert [48], [49]; electronic-record requirements under the BSA [45]. Validated methods and practitioner competence are emphasized by the UK regulator [52]. Through TFLA, chronology and attribution risks from inconsistent IoT timestamps are linked to cross-source correlation; reliability and due-process concerns from opaque AI results are linked to validation, version records, independent verification, and disclosure.

7.3 Framework logic and worked application

The six-layer sequence and feedback for additional collection or validation are shown (Figure 6). In a hypothetical cloud-account-compromise investigation, provider logs, IP records, metadata, and exported files are examined through AI-based flagging of anomalous logins. The cloud platform and AI system are identified under Technology; primary provider records are distinguished from derived anomaly scores under Evidence Source. Forensic Challenges are provider control, missing or inconsistent timestamps, incomplete exports, false positives, and opaque model decisions.

Cross-border authority, privacy, authentication, attribution, and contestability are addressed under Legal Risks; provenance, integrity, relevance, reliability, and actor linkage are addressed under Admissibility Requirements. Governance Responses are documented authority and exports, package hashing, independent timeline correlation, model/version records, source-level verification, and disclosed limitations. Independently authenticated records need not be invalidated by unvalidated AI conclusions; unlawfully obtained or inadequately authenticated sources cannot be repaired through accurate analysis. Application is illustrated by United States v. Vayner [51].

Figure 6. Technology–forensic–legal admissibility framework

Table 7. Operational Layers of the TFLA Framework

Layer	Core Question	Main Evidence/Criteria	Output
Technology	By what system was the evidence produced or affected?	Platform, provider, version, configuration	Technology profile
Evidence Source	What primary or derived evidence is available?	Files, logs, metadata, outputs, telemetry	Evidence profile
Forensic Challenge	By what factors can technical reliability be reduced?	Volatility, opacity, clock error, attribution uncertainty	Forensic risk statement
Legal Risk	What legal consequence may be created?	Privacy, jurisdiction, due process, accountability	Legal risk statement
Admissibility	What must be demonstrated?	Authenticity, integrity, reliability, relevance, attribution	Evidentiary assessment
Governance Response	By what safeguard is the risk addressed?	Validation, corroboration, standards, auditability, oversight	Required control

Technology was a social media platform; Evidence Source was a profile attributed to the defendant. Creator/controller identification was required (Forensic Challenge), with unreliable attribution and insufficient authentication as Legal Risks. Profile attribution to the alleged user, not mere capture, was required (Admissibility Requirement). Under Governance Response, legally sufficient attribution would be supported through TFLA-directed account, device, network, platform, communication, or contextual corroboration. Evidence-generating technology, claim-supporting primary or derived artifacts, technical weaknesses, legal consequences, evidentiary requirements, and controls required before reliance are assessed.

7.4 Contribution, scope, and validation requirements

Technical weaknesses are translated into legal consequences, primary evidence separated from analytical outputs, and evidentiary concerns linked with safeguards. Analytical layers are preserved through technology neutrality; controls can be varied across cloud, LLM, blockchain, and cryptographic environments. Documentation and corroboration may be structured by investigators; reliability claims' basis and limits examined by legal practitioners; principles connected with operational controls by policymakers. TFLA is conceptual, not empirically validated or legally binding. Statutes, judicial discretion, forensic standards, and expert evaluation are not replaced. Usability, risk-identification completeness, inter-examiner consistency, and technical/legal decision agreement should be assessed across controlled and real-world scenarios (Section 8).

8. Research gaps and future directions

Shared authentication, expert-reliability, automated-evidence, and cross-border access principles should be comparatively examined, with jurisdiction-specific privacy and due-process safeguards preserved. Tool benchmarking, version control, error reporting, metadata/timestamp verification, and provider-export traceability are prioritized for empirical research. Prompt/model logging, source verification, consistency assessment, and hallucination reporting are required for LLM studies [31]; cross-source and timeline evaluation for anti-forensic detection. Blockchain heuristic accuracy and false attribution should be quantified [32,33]. Provenance-preserving cryptographic migration, re-attestation, and renewed timestamps should be examined for long-term preservation [57-60]. Privacy, bias, professional competence, judicial training, and cooperation are institutional research priorities. TFLA usability, risk coverage, inter-examiner consistency, and technical/legal agreement should be tested through controlled datasets, simulated investigations, and reported cases across jurisdictions and technologies.

9. Limitations of the review

Secondary literature and authoritative documents were used, not interviews, surveys, observation, or experiments. Findings and TFLA were interpreted, not empirically validated. Selection and interpretation bias are permitted, and statistical aggregation is precluded by structured narrative design, heterogeneous sources, and the absence of independent duplicate coding or inter-rater assessment.

The review is bounded by database coverage, publication window, language accessibility, inclusion criteria, and search strategy; relevant sources may have been missed. The 60-source corpus is distinguished from supplementary clarification authorities. Longevity is limited by rapid technological change; uniform application by jurisdictional differences. Section 8's comparative, practitioner-oriented, and empirical-validation priorities are motivated by these constraints.

10. Conclusion

Cybercrime law must be connected with forensic systems for distributed, dynamic, automated, and provider-controlled evidence through digital-evidence governance. Technical integrity is necessary but distinct from legal admissibility. Authorship is not established by hashes; metadata must be corroborated; automated conclusions validated and source-verified; human identity is not established by transaction visibility. Cryptographic agility is required for long-term trust. Technology, Evidence Source, Forensic Challenge, Legal Risk, Admissibility Requirement, and Governance Response are connected through TFLA. Technical weaknesses are translated into legal consequences and safeguards; standards or legal tests are not replaced. Documented methods, validated tools, corroboration, oversight, competence, and cooperation are required for technology-neutral, technically informed governance. Conceptual integration is proposed through TFLA, pending empirical evaluation.

Ethical issue

The authors are aware of and comply with best practices in publication ethics, specifically regarding authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with research ethics policies. The authors adhere to publication requirements that the submitted work is original and has not been published elsewhere. All survey participants provided informed consent before participating, and the anonymity and confidentiality of all respondents were strictly maintained throughout the research process.

Data availability statement

The manuscript contains all the data. However, additional data will be provided by the corresponding author upon reasonable request.

Conflict of interest

The authors declare no potential conflict of interest.

References

[1] R. K. Bharati, P. G. Khodke, C. P. Khadilkar, and S. K. Bawiskar, "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings," International Journal of Scientific Research in Science and Technology, vol. 11, no. 16, pp. 24–35, 2024. Publisher record verified; SSRN version DOI: 10.2139/ssrn.4896874.

[2] E. Arjun and P. Singh, "Future Directions in Digital Forensics and Cybersecurity," in Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics, Wiley, 2025, pp. 333–365. doi: 10.1002/9781394268917.ch15.

[3] Jaddoa and K. Ainscough, "From Devices to the Dock: Challenges in the Legal Admissibility of IoT Evidence," in Proc. 12th Int. Conf. Future Internet of Things and Cloud (FiCloud), 2025, pp. 467–476. doi: 10.1109/FiCloud66139.2025.00071.

[4] S. Katkuri, "Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India," Indian Journal of Public Administration, vol. 71, no. 1, pp. 75–91, 2025. doi: 10.1177/00195561241284886.

[5] AlMutawa, R. A. Ikuesan, and H. Said, "Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model," Future Internet, vol. 16, no. 12, Art. no. 437, 2024. doi: 10.3390/fi16120437.

[6] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response," Forensic Science International: Digital Investigation, vol. 48, Art. no. 301675, 2024. doi: 10.1016/j.fsidi.2023.301675.

[7] R. Thakur, S. Kumar, S. K. Singh, K. Singla, S. K. Sharma, and V. Arya, "Cyber Synergy: Unlocking the Potential Use of Biometric Systems and Multimedia Forensics in Cybercrime Investigations," in Digital Forensics and Cyber Crime Investigation: Recent Advances and Future Directions, CRC Press, 2024, pp. 241–267. doi: 10.1201/9781003207573-12.

[8] D. B. Ferreira and E. A. Gromova, "Digital Evidence: The Admissibility of Leaked and Hacked Evidence in Arbitration Proceedings," International Journal for the Semiotics of Law, vol. 37, no. 3, pp. 903–922, 2024. doi: 10.1007/s11196-023-10014-1.

[9] M. Sharma, R. K. Kohli, and K. Sharma, "Tomorrow's Shields: Exploring Future Trends in Cyber Security and Forensics," in Securing the Digital Frontier, Wiley, 2025, pp. 367–385. doi: 10.1002/9781394268917.ch16.

[10] N. Alsaraireh, "Digital Forensics in the Age of Cybercrime: Challenges and Future Directions," in Tech Fusion in Business and Society, vol. 2, Springer Nature, 2025, pp. 555–564. doi: 10.1007/978-3-031-84636-6_48.

[11] P. Jain, P. Verma, T. Debnath, L. Heisnam, S. Chaudhary, and S. Balouria, "Cybersecurity Forensics with AI: A Comprehensive Review," in Quantum Computing: The Future of Information Processing, Auerbach/CRC Press, 2025, pp. 170–184. doi: 10.1201/9781003499459-10.

[12] R. Stoykova, "A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings," Computer Law & Security Review, vol. 55, Art. no. 106040, 2024. doi: 10.1016/j.clsr.2024.106040.

[13] U. M. Mohammed, A. E. Omolara, O. I. Abiodun, J. Rasheed, O. Osman, P. M. Lar, P. O. Adeyinka, and A. G. Olugbenga, "Cyber Threat in Drone Systems: Bridging Real-Time Security, Legal Admissibility, and Digital Forensic Solution Readiness," Frontiers in Communications and Networks, vol. 6, Art. no. 1661928, 2025. doi: https://doi.org/10.3389/frcmn.2025.1661928.

[14] R. Stoykova, "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations," Computer Law & Security Review, vol. 49, Art. no. 105801, 2023. doi: 10.1016/j.clsr.2023.105801.

[15] W. Shafik, A. Tufail, R. A. A. H. M. Apong, and S. Balasubramaniam, "Future Directions in Cybersecurity, Digital Forensics and Biometric Systems," in AI Based Advancements in Biometrics and its Applications, CRC Press, 2024, pp. 238–263. doi: 10.1201/9781032702377-13.

[16] H. Zhang and X. Gong, "The Research on an Electronic Evidence Forensic System for Cross-Border Cybercrime," International Journal of Evidence & Proof, vol. 28, no. 1, pp. 21–44, 2024. doi: 10.1177/13657127231187059.

[17] R. Jain and B. Sonowal, "Analyzing the Procedure for Investigation in Cybercrime and Admissibility of Electronic Evidence," in Cybercrime Unveiled: Technologies for Analysing Legal Complexity, Springer, 2025, pp. 265–289. doi: 10.1007/978-3-031-80557-8_12.

[18] Singh and A. Raj, "Convergence of Digital Forensics and Intelligent Data in Cyberspace," in Proceedings of the International Conference on Computing and Communication Systems for Industrial Applications, Springer Nature, 2024, pp. 111–119. doi: 10.1007/978-981-97-5862-3_9.

[19] G. Tiwari, K. Pandey, M. Desai, V. Musale, D. Wategaonkar, and M. Bedekar, "The Legal and Ethical Crossroads of Artificial Intelligence in Cybersecurity and Digital Forensics," in Digital Defence: Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics, CRC Press, 2025, pp. 93–110. doi: https://doi.org/10.1201/9781032714813-6.

[20] P. Pappachan, N. S. Adi, G. Firmansyah, and M. Rahaman, "Deep Learning-Based Forensics and Anti-Forensics," in Digital Forensics and Cyber Crime Investigation: Recent Advances and Future Directions, CRC Press, 2024, pp. 211–240. doi: 10.1201/9781003207573-11.

[21] R. Stoykova, S. Andersen, K. Franke, and S. Axelsson, "Reliability Assessment of Digital Forensic Investigations in the Norwegian Police," Forensic Science International: Digital Investigation, vol. 40, Art. no. 301351, 2022. doi: 10.1016/j.fsidi.2022.301351.

[22] W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges," Sensors, vol. 24, no. 2, Art. no. 433, 2024. doi: 10.3390/s24020433.

[23] Ala'a Saeb Al-Sherideh, Samah Suleiman Al-Zou'bi, Fuad Alshraiedeh, Esraa Abu Elsoud, Suha Afaneh, Mohammad Rasmi Al-Mousa, Raed Alazaidah, Mohammed Khouj, and Ghassan Samara, "Digital Evidence and Forensic Tools in Cyber Law: A Comprehensive Analysis," in Proc. 25th International Arab Conference on Information Technology (ACIT),

IEEE, 2024, pp. 1–6. doi: https://doi.org/10.1109/ACIT62805.2024.10877028

[24] Sachoulidou, "Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation," New Journal of European Criminal Law, vol. 15, no. 3, pp. 256–274, 2024. doi: 10.1177/20322844241258649.

[25] F. M. Ibrahim, H. Alawsi, and M. N. Mohammed, "The Evolution of Cybercrime: Challenges and Advancements in Digital Forensics," in Tech Fusion in Business and Society, vol. 2, Springer Nature, 2025, pp. 455–464. doi: 10.1007/978-3-031-84636-6_39.

[26] R. Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," Computer Law & Security Review, vol. 42, Art. no. 105575, 2021. doi: 10.1016/j.clsr.2021.105575.

[27] M. Rojszczak, "e-Evidence Cooperation in Criminal Matters from an EU Perspective," The Modern Law Review, vol. 85, no. 4, pp. 997–1028, 2022. doi: 10.1111/1468-2230.12749.

[28] N. Allah Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," Mexican Law Review, vol. 16, no. 2, pp. 23–54, 2024. doi: 10.22201/iij.24485306e.2024.2.18892.

[29] S. Sethu Laksmi, L. Das, R. S. R. Khan, and P. Chakraborty, "Emerging Threats and Trends in Digital Forensics and Cybersecurity," in Emerging Threats and Countermeasures in Cybersecurity, Wiley, 2025, pp. 1–21. doi: 10.1002/9781394230600.ch1.

[30] Gascón Marcén, "The Push for the International Regulation of Cross-Border Access to Electronic Evidence and Human Rights," Cuadernos de Derecho Transnacional, vol. 15, no. 1, pp. 385–402, 2023. doi: 10.20318/cdt.2023.7545.

[31] J. P. Khatiwala, D. K. N. Addai, and W. Xu, "Evaluating the Reliability of Digital Forensic Evidence Discovered by Large Language Model: A Case Study," in Proc. 49th IEEE Annual Computers, Software, and Applications Conference (COMPSAC), 2025, pp. 1067–1076. doi: 10.1109/COMPSAC65507.2025.00138.

[32] S. Dudani, I. Baggili, D. Raymond, and R. Marchany, "The Current State of Cryptocurrency Forensics," Forensic Science International: Digital Investigation, vol. 46, Art. no. 301576, 2023. doi: 10.1016/j.fsidi.2023.301576.

[33] T. Thomas, T. Edwards, and I. Baggili, "BlockQuery: Toward Forensically Sound Cryptocurrency Investigation," Forensic Science International: Digital Investigation, vol. 40, Art. no. 301340, 2022. doi: 10.1016/j.fsidi.2022.301340.

[34] ISO/IEC, ISO/IEC 27037:2012, Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva, Switzerland: International Organization for Standardization, 2012. [Online]. Available: https://www.iso.org/standard/44381.html.

[35] ISO/IEC, ISO/IEC 27041:2015, Information Technology - Security Techniques - Guidance on Assuring Suitability and Adequacy of Incident Investigative Method. Geneva, Switzerland: International Organization for Standardization, 2015. [Online]. Available: https://www.iso.org/standard/44405.html.

[36] ISO/IEC, ISO/IEC 27042:2015, Information Technology - Security Techniques - Guidelines for the Analysis and Interpretation of Digital Evidence. Geneva, Switzerland: International Organization for Standardization, 2015. [Online]. Available: https://www.iso.org/standard/44406.html.

[37] ISO/IEC, ISO/IEC 27043:2015, Information Technology - Security Techniques - Incident Investigation Principles and Processes. Geneva, Switzerland: International Organization for Standardization, 2015. [Online]. Available: https://www.iso.org/standard/44407.html.

[38] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2006. doi: https://doi.org/10.6028/NIST.SP.800-86.

[39] R. Ayers, S. Brothers, and W. Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1. Gaithersburg, MD, USA: National Institute of Standards and Technology, May 2014. doi: https://doi.org/10.6028/NIST.SP.800-101r1.

[40] Scientific Working Group on Digital Evidence (SWGDE), Best Practices for Digital Evidence Collection, SWGDE 18-F-002-2.0, Version 2.0. SWGDE, 2025. [Online]. Available: https://www.swgde.org/documents/published-complete-listing/18-f-002-2-0/.

[41] Scientific Working Group on Digital Evidence (SWGDE), Best Practices for Computer Forensic Acquisition, SWGDE 17-F-002-2.1, Version 2.1. SWGDE, 2023. [Online]. Available: https://www.swgde.org/documents/published-complete-listing/17-f-002-2-1/.

[42] Council of Europe, Convention on Cybercrime, European Treaty Series No. 185. Budapest, Hungary: Council of Europe, Nov. 23, 2001. [Online]. Available: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[43] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, Council of Europe Treaty Series No. 224. Strasbourg, France: Council of Europe, May 12, 2022. [Online]. Available: https://www.coe.int/en/web/cybercrime/second-additional-protocol.

[44] European Parliament and Council of the European Union, "Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings," Official Journal of the European Union, L 191, pp. 118–180, Jul. 28, 2023. [Online]. Available:

https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng.
[45] Government of India, The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023, Gazette of India, Dec. 25, 2023. Ministry of Home Affairs, Government of India. [Online]. Available: https://www.indiacode.nic.in/indiacode/handle/123456789/20063?view_type=browse.
[46] Supreme Court of India, Anvar P.V. v. P.K. Basheer & Ors., Civil Appeal No. 4226 of 2012, (2014) 10 SCC 473, decided Sept. 18, 2014. [Online]. Available: https://indiankanoon.org/doc/187283766/.
[47] Supreme Court of India, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., Civil Appeal Nos. 20825–20826 of 2017, (2020) 7 SCC 1, decided Jul. 14, 2020. [Online]. Available: https://indiankanoon.org/doc/172105947/.
[48] United States Courts, Federal Rules of Evidence, Rules 702, 901, 902(13), and 902(14), United States, as amended through 2024. [Online]. Available: https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence.
[49] Supreme Court of the United States, Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), decided Jun. 28, 1993. United States Reports, vol. 509, p. 579. Washington, DC: U.S. Government Publishing Office. [Online]. Available: https://www.govinfo.gov/app/details/USREPORTS-509/USREPORTS-509-579.
[50] United States Court of Appeals for the District of Columbia, Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923). [Online]. Available: https://www.mass.gov/doc/frye-v-united-states-293-f-1013-dc-cir-1923/download.
[51] United States Court of Appeals for the Second Circuit, United States v. Vayner, 769 F.3d 125, Docket No. 13-803-cr, decided Oct. 3, 2014. [Online]. Available: https://www.govinfo.gov/content/pkg/USCOURTS-ca2-13-00803/pdf/USCOURTS-ca2-13-00803-0.pdf.
[52] Forensic Science Regulator and Home Office, Forensic Science Activities: Statutory Code of Practice, Version 2. London, United Kingdom, 2025. [Online]. Available: https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2.
[53] Q. H. Dang, Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2015. doi: https://doi.org/10.6028/NIST.FIPS.180-4.
[54] M. J. Dworkin, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Federal Information Processing Standards Publication 202. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2015. doi: https://doi.org/10.6028/NIST.FIPS.202.
[55] S. Turner and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms," Internet Engineering Task Force, RFC 6151, pp. 1–7, Mar. 2011. doi: https://doi.org/10.17487/RFC6151.
[56] National Institute of Standards and Technology, "NIST Transitioning Away from SHA-1 for All Applications," Dec. 15, 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/12/nist-transitioning-away-sha-1-all-applications.
[57] National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, Federal Information Processing Standards Publication 203. Gaithersburg, MD, USA: NIST, Aug. 2024. doi: https://doi.org/10.6028/NIST.FIPS.203.
[58] National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, Federal Information Processing Standards Publication 204. Gaithersburg, MD, USA: NIST, Aug. 2024. doi: https://doi.org/10.6028/NIST.FIPS.204.
[59] National Institute of Standards and Technology, Stateless Hash-Based Digital Signature Standard, Federal Information Processing Standards Publication 205. Gaithersburg, MD, USA: NIST, Aug. 2024. doi: https://doi.org/10.6028/NIST.FIPS.205.
[60] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, Report on Post-Quantum Cryptography, NIST Interagency/Internal Report 8105. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016. doi: https://doi.org/10.6028/NIST.IR.8105.