Law and Digital Forensics: Evidentiary Standards, Chain of Custody, and Admissibility in the Digital Age

Disha Dogra[1*]
[1]Assistant Professor, Amity Law School Amity University, Mohali, India

* Corresponding Author- dishadogra85@gmail.com

Abstract: Digital forensics has become one of the most important pillars of contemporary evidence practice. Courts, investigators, regulators, and private litigants increasingly depend on electronically stored information, device artifacts, metadata, communication records, cloud logs, and network traces to prove or disprove facts in dispute. Yet digital evidence presents legal and technical complications that are far more intricate than those associated with traditional physical evidence. Issues relating to authenticity, admissibility, integrity, chain of custody, lawful acquisition, and expert testimony frequently determine whether evidence is accepted, challenged, or excluded. This paper examines the intersection of law and digital forensics through a detailed doctrinal and analytical framework. It reviews the legal foundations governing electronic evidence, explains forensic procedures that protect evidentiary value, and analyzes common courtroom disputes arising from digital investigations. The study further evaluates practical difficulties such as encryption, cloud storage, cross-border jurisdiction, overcollection, tool validation, and the communication gap between forensic experts and legal decision-makers. The paper argues that legal admissibility depends not only on technical accuracy but on transparent, documented, and proportionate forensic practice. It concludes by proposing recommendations for investigators, legal professionals, and policymakers aimed at improving the reliability and courtroom usefulness of digital evidence.

Keywords: Digital evidence, digital forensics, chain of custody, admissibility, authenticity, expert witness, cyber law, evidence integrity, electronic records.

1. Introduction

The digitization of communication, commerce, and record-keeping has fundamentally altered the landscape of criminal activity. Offenses ranging from financial fraud and identity theft to child exploitation, ransomware, and state-sponsored intrusion now leave traces primarily in electronic rather than physical form. Digital forensics has emerged as the scientific discipline tasked with recovering, preserving, and interpreting these traces so that they can withstand legal scrutiny. Unlike traditional forensic sciences, digital forensics must contend with evidence that is intangible, volatile, easily altered, and often distributed across multiple jurisdictions and service providers.

Law, in turn, has struggled to keep pace with the velocity of technological change. Statutes drafted for physical searches and tangible property must be reinterpreted, or entirely rewritten, to accommodate cloud storage, encrypted communications, and data that may reside outside the territorial jurisdiction of the investigating authority. The admissibility of digital evidence in court depends not merely on its technical accuracy but on compliance with procedural rules governing search and seizure, authentication, and the chain of custody.

The stakes of getting this relationship right are considerable. Overly permissive investigative practice risks violating constitutional protections against unreasonable search and seizure, chilling legitimate use of encryption and cloud services, and producing evidence that courts later exclude, wasting investigative resources and undermining public confidence. Conversely, overly restrictive procedural requirements, divorced from the operational realities of volatile, distributed, and encrypted data, risk allowing serious crimes to go unpunished simply because evidence could not be captured before it degraded or because jurisdictional friction delayed access beyond usefulness. Calibrating this balance requires sustained dialogue between technologists who understand what is forensically possible and legislators and judges who must translate that possibility into enforceable, rights-respecting rules.

This paper provides a structured examination of the relationship between digital forensics and law, drawing on statutory text, appellate case law, international treaties, and technical standards. Section II describes the digital forensic investigation process and the taxonomy of digital evidence. Section III surveys the legal frameworks that govern this process across representative jurisdictions. Section IV discusses evidentiary admissibility standards and the treatment of algorithmic and AI-assisted findings. Section V details chain-of-custody requirements and the consequences of procedural lapses. Section VI analyzes prevailing challenges, including jurisdiction, encryption, and tool validation. Section VII presents illustrative case studies drawn from multiple legal systems. Section VIII considers emerging technologies and their doctrinal implications, Section IX offers recommendations for practitioners and policymakers, and Section X concludes the paper.

2. Digital forensics: concepts and process

Digital forensics is commonly defined as the application of scientific methods to the identification, collection, preservation, examination, and presentation of digital evidence in a manner that maintains its integrity and evidentiary value.[1] The discipline spans several sub-domains, including computer forensics, network forensics, mobile device forensics, cloud forensics, and memory forensics, each addressing distinct sources and challenges of evidence acquisition.

2.1 Investigation Lifecycle

Although terminology varies across standards bodies such as the National Institute of Standards and Technology (NIST) [2] and the International Organization for Standardization (ISO/IEC 27037), [3] the forensic process is generally represented as a sequential lifecycle. Fig. 1 illustrates the seven-stage model adopted in this paper.

Fig. 1. Digital forensic investigation process, from identification through presentation

During identification, potential sources of evidence—servers, endpoints, mobile devices, IoT sensors, or cloud accounts—are located and their evidentiary relevance assessed. Preservation ensures that volatile data, such as system memory or active network connections, is captured before alteration or loss occurs. Collection involves the forensically sound acquisition of data, typically through bit-for-bit imaging accompanied by cryptographic hashing (e.g., SHA-256) to demonstrate that the copy is identical to the original. Examination applies systematic techniques to extract relevant artifacts, while analysis interprets those artifacts to reconstruct events and establish attribution. Documentation records every action taken throughout the process, and presentation communicates findings to investigators, attorneys, or the court in a comprehensible and defensible manner.

2.2 Categories of Digital Evidence

Digital evidence may originate from computers and storage media, mobile devices, network traffic, cloud-hosted services, and embedded or IoT devices. Each category presents distinct acquisition constraints: cloud evidence, for example, may require cooperation from a third-party provider and raises jurisdictional questions [4], while mobile devices increasingly employ hardware-backed encryption that limits forensic access without vendor assistance or specialized exploitation tools. Network evidence is often the most transient of all categories, since packet captures and flow logs may be retained for only days or weeks absent a preservation request, making rapid legal process essential to prevent irretrievable loss.

2.3 Core Forensic Principles

Regardless of sub-domain, digital forensic practice is grounded in a small set of guiding principles that also underpin legal acceptance of the resulting evidence. First, the principle of minimal intervention requires that the acquisition process alter the original data as little as possible, typically achieved by working from a verified forensic image rather than the source device itself. Second, the principle of documentation requires a complete, contemporaneous record of every action taken, enabling independent reproduction and review. Third, the principle of competence requires that only individuals with appropriate training and demonstrable proficiency perform forensic acquisition and analysis, since courts increasingly scrutinize examiner qualifications during admissibility challenges. Fourth, the principle of auditability requires that tools and methods be transparent enough that a second examiner, given the same data, could reach and verify the same conclusions. These principles collectively bridge the technical and legal domains: a forensically sound process is, almost by definition, one that a court can trust

3. Legal frameworks governing digital forensics

The legal treatment of digital forensics operates across three interacting layers: international instruments that promote harmonization and cross-border cooperation, national legislation that defines offenses and investigative powers, and procedural or evidentiary rules that govern how evidence is gathered, preserved, and admitted in court. Fig. 2 depicts this layered structure.

Fig. 2. Layered legal framework governing digital forensic practice.

3.1 International Instruments

The Council of Europe's Convention on Cybercrime (the Budapest Convention) [5] remains the principal multilateral treaty addressing cybercrime and digital evidence, establishing common definitions of offenses and procedural powers, and creating a framework for mutual legal assistance. Mutual Legal Assistance Treaties (MLATs) supplement this framework but are frequently criticized for the length of time required to execute cross-border evidence requests, prompting newer mechanisms such as the U.S. CLOUD Act [6] and the EU's e-Evidence framework,[7] which permit more direct requests to service providers.

3.2 National Legislation

National statutes translate international commitments into enforceable domestic law and vary considerably in scope and procedural detail.[8]-[13] Table I summarizes representative legislative instruments in four jurisdictions.

Jurisdiction	Principal Legislation	Investigative Powers	Evidentiary Provisions
United States	Computer Fraud and Abuse Act (CFAA); Federal Rules of Evidence; ECPA	Search warrants under Fed. R. Crim. P. 41; CLOUD Act for cross-border data	Authentication under FRE 901/902(13)-(14); Daubert standard for expert testimony
United Kingdom	Computer Misuse Act 1990; Police and Criminal Evidence Act (PACE) 1984	PACE search and seizure powers; production orders	PACE s.69 (repealed) replaced by presumption of proper functioning of computers
European Union	GDPR; NIS2 Directive; e-Evidence Regulation	European Production and Preservation Orders (EPOC)	Member-state evidentiary rules; data protection compliance in collection
India	Information Technology Act, 2000 (amended 2008); Bharatiya Sakshya Adhiniyam, 2023	Search/seizure under Cr.P.C. successor BNSS; s.79A examiner certification	Certificate under s.63 BSA (formerly s.65B Evidence Act) for electronic records

Table-1 Comparative Overview of National Digital Forensic and Cyber Law Instruments

3.3. Procedural and Evidentiary Rules

Procedural rules govern the mechanics of search, seizure, and evidence handling, and are typically the layer most directly implicated in forensic practice. Warrant requirements, particularity of description, and limits on the scope of a search are central constitutional or statutory safeguards intended to prevent overbroad access to personal data, an especially acute concern given the volume and sensitivity of information contained in a single smartphone or cloud account. Many jurisdictions now require that a warrant specify not only the device to be searched but also the categories of data and the time period sought, and courts have increasingly invalidated warrants that authorize an unlimited search of an entire device without such particularity.

3.4 Data Protection and Privacy Law

A distinct but overlapping body of law governs the protection of personal data independent of any criminal investigation, and it frequently constrains how forensic evidence may be collected, processed, and retained even by law enforcement. The EU's General Data Protection Regulation (GDPR) [11] permits processing for law enforcement purposes primarily under a parallel instrument, the Law Enforcement Directive, but still requires proportionality, purpose limitation, and, in many member states, judicial authorization before bulk data is accessed. Similar tensions arise under sectoral privacy statutes in the United States, such as the Stored Communications Act, [14] which distinguishes between content and non-content data and imposes different disclosure thresholds accordingly. Forensic practitioners must therefore treat privacy compliance not as a separate concern from evidentiary admissibility but as a precondition for it, since evidence obtained in violation of data protection law may be excluded on public-policy grounds even where it is technically authentic and reliable.

4. Digital evidence and admissibility

For digital evidence to influence the outcome of a legal proceeding, it must satisfy jurisdiction-specific admissibility criteria. While formulations differ, most legal systems converge on four core requirements: relevance, authenticity, reliability, and compliance with procedural safeguards during acquisition.

Authenticity requires that the proponent demonstrates the evidence is what it purports to be, typically established through hash verification, metadata analysis, and testimony describing the acquisition method. Reliability concerns the soundness of the tools and techniques used; many jurisdictions apply a standard analogous to the Daubert or Frye tests, [15] examining whether a forensic method has been tested, subjected to peer review, has a known error rate, and is generally accepted within the professional community. Table II compares admissibility standards across jurisdictions discussed in this paper.

Jurisdiction	Governing Standard	Key Requirement
United States	Federal Rules of Evidence 901, 902; Daubert v. Merrell Dow	Authentication plus scientific reliability of forensic method
United Kingdom	Common law presumption of proper functioning; PACE Codes	Reliability of automated systems generally presumed absent contrary evidence
India	Bharatiya Sakshya Adhiniyam s.63 (successor to Evidence Act s.65B)	Mandatory certificate identifying device and manner of production
European Union	Member-state civil/criminal codes; GDPR compliance	Evidence must be lawfully obtained; unlawful processing may bar admission

Table 2 Admissibility Standards for Digital Evidence

A recurring point of contention is the treatment of evidence obtained through automated or algorithmic processes, including artificial intelligence-assisted analysis. Courts increasingly require disclosure of the underlying methodology so that opposing counsel may challenge its reliability, a requirement that places growing emphasis on the explainability and validation of forensic software. Where a forensic tool has been independently validated through peer-reviewed testing and its source or configuration is available for inspection, courts have generally been receptive to its output; where a tool operates as a proprietary black box with undisclosed internal logic, some courts have expressed skepticism, particularly in high-stakes criminal matters, invoking the defendant's right to confront the evidence against them.

A second recurring issue concerns hearsay treatment of machine-generated records, such as system logs or metadata that were never authored by a human declarant. Most common-law jurisdictions treat such records as falling outside the traditional hearsay rule precisely because they are not human assertions, though the proponent must still establish that the generating system functioned reliably at the relevant time. Civil-law jurisdictions typically address the same concern through rules on documentary evidence and expert certification rather than hearsay doctrine as such, but the underlying reliability inquiry is functionally similar.

5. Chain of custody

Chain of custody refers to the chronological documentation that traces the seizure, custody, control, transfer, analysis, and disposition of evidence. For digital evidence, this record must capture not only physical custody of storage media but also every operation performed on the data, since digital artifacts can be modified without leaving visible traces unless cryptographic controls are used. Fig. 3 depicts the cyclical documentation process typically required to preserve evidentiary integrity from seizure through eventual disposal or archival.

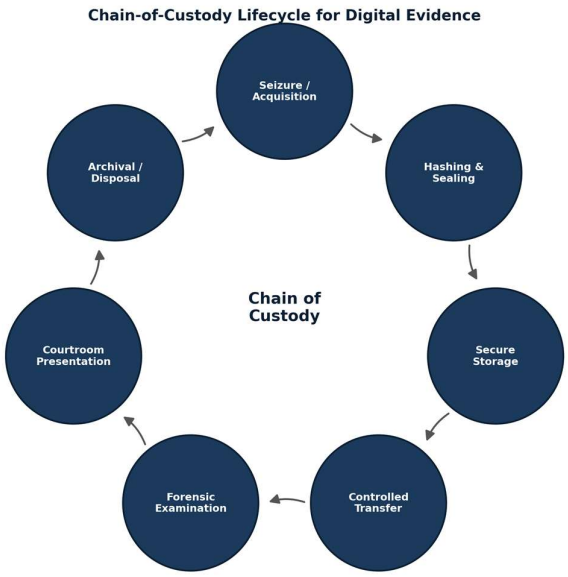

Fig. 3. Chain-of-custody lifecycle for digital evidence

A defensible chain of custody typically includes a documented log of who accessed the evidence, when, for what purpose, and using which tools, supported by cryptographic hash values computed at acquisition and re-verified at each subsequent stage. A break in this chain, whether through undocumented access, hash mismatch, or unexplained gaps in custody, can result in evidence being excluded or its weight substantially diminished, regardless of its underlying probative value.

In practice, chain-of-custody disputes rarely allege that evidence was deliberately fabricated; far more commonly, they arise from administrative lapses such as a missing signature on a transfer log, an evidence locker accessible to unauthorized personnel, or a forensic workstation whose write-blocking hardware was not verified before imaging. Because these lapses are often preventable through routine laboratory accreditation and standard operating procedures, jurisdictions that have invested in accredited digital forensic laboratories, such as those certified under ISO/IEC 17025, [16] report markedly fewer successful chain-of-custody challenges than those relying on ad hoc departmental practices. This suggests that investment in laboratory infrastructure and procedural discipline yields direct benefits in courtroom outcomes, independent of any improvement in underlying investigative technique.

6. Challenges at the intersection of forensics and law

6.1 Jurisdiction and Cross-Border Data

Data relevant to an investigation frequently resides on servers located outside the investigating jurisdiction or is fragmented across multiple cloud regions for redundancy. Traditional MLAT processes can take months, during which volatile evidence may be lost or altered, prompting unilateral assertions of extraterritorial jurisdiction that themselves raise sovereignty concerns.

6.2 Encryption and Anti-Forensic Techniques

Strong end-to-end encryption, full-disk encryption, and deliberate anti-forensic measures such as data wiping, steganography, and log manipulation impede evidence recovery. The resulting policy debate over mandated backdoors or key-escrow mechanisms remains unresolved, with security researchers generally cautioning that any exceptional access mechanism weakens security for all users.

6.3 Volume, Volatility, and Cloud/IoT Evidence

The sheer volume of data generated by modern systems, combined with the volatility of information such as RAM contents or ephemeral container instances, complicates timely and complete evidence preservation.[23] Internet-of-Things devices further diversify data formats and storage architectures, often lacking standardized forensic interfaces.

6.4 Standardization and Tool Validation

Although frameworks such as ISO/IEC 27037,[3] 27041,[21] and 27042 [22] provide guidance on evidence handling and tool validation, adoption is inconsistent, and many jurisdictions lack accreditation regimes for forensic laboratories or practitioners, creating variability in the reliability of results presented in court.

6.5 Workforce Capacity and Resource Constraints

Beyond technical and doctrinal obstacles, many law enforcement agencies face a persistent shortage of trained digital forensic examiners relative to the volume of devices requiring analysis, resulting in evidence backlogs that can extend investigative and pretrial timelines by months or years. Smaller jurisdictions and developing economies face this constraint acutely, often lacking both the specialized software licenses and the sustained training pipelines necessary to build in-house capability, and consequently relying on centralized national laboratories or private contractors whose availability may itself become a bottleneck in time-sensitive matters.

Table III summarizes representative forensic tool categories referenced throughout the literature, illustrating the breadth of technical capability that legal practitioners must be able to evaluate when assessing the reliability of forensic findings.

Category	Representative Tools	Primary Legal Relevance
Disk / Image Acquisition	EnCase, FTK Imager, dd/dcfldd	Establishes forensically sound copy for authentication under evidentiary rules
Mobile Forensics	Cellebrite UFED, Magnet AXIOM	Raises search-scope and encryption-access legal questions
Network Forensics	Wireshark, NetworkMiner	Supports attribution; implicates wiretap/interception statutes
Memory Forensics	Volatility, Rekall	Captures volatile evidence; timing of capture affects reliability
Cloud Forensics	Provider APIs, Magnet AXIOM Cloud	Implicates cross-border data requests and provider terms of service

Table 3 Representative Digital Forensic Tool Categories

7. Illustrative case studies

7.1 Riley v. California (2014)

The U.S. Supreme Court held that police generally require a warrant to search the digital contents of a cell phone seized incident to arrest, recognizing that modern smartphones contain a quantity and quality of personal information fundamentally different from physical items traditionally subject to search-incident-to-arrest exceptions.[17] The decision illustrates courts' growing recognition that digital evidence demands distinct constitutional treatment.

7.2 Anvar P.V. v. P.K. Basheer (2014, India)

The Supreme Court of India clarified that a certificate under the Evidence Act (subsequently reformulated in the Bharatiya Sakshya Adhiniyam) is a mandatory precondition for the admissibility of electronic records produced from a computer, reversing earlier appellate interpretations that had permitted oral evidence to substitute for the statutory certificate.[18] This case underscores the strict procedural formalism many jurisdictions apply to digital evidence.

7.3 Microsoft Corp. v. United States (2018, mooted by CLOUD Act)

This dispute over whether U.S. law enforcement could compel a domestic provider to produce data stored on a server in Ireland was rendered moot by the enactment of the CLOUD Act, which clarified that U.S. warrants extend to data controlled by U.S.-based providers regardless of physical storage location, subject to comity considerations and bilateral executive agreements with partner nations.[19]

7.4 R. V. Vu (2013, Canada)

The Supreme Court of Canada held that a warrant authorizing the search of a residence does not, without more, authorize the search of computers found within it, reasoning that computers implicate a heightened privacy interest distinct from other household objects and therefore require specific judicial authorization before their contents may be examined.[20] The decision parallels the reasoning later adopted in Riley and reflects a broader judicial trend of treating digital devices as categorically different from traditional containers for search-and-seizure purposes.

8. Emerging technologies and future directions

Artificial intelligence and machine learning are increasingly deployed for triage of large evidence sets, anomaly detection in network logs, and multimedia authentication (e.g., detecting deepfakes). Their use raises legal questions concerning explainability, since a black-box classification may not satisfy reliability standards requiring that a method's error rate and methodology be articulable to a court.

Blockchain-based evidence management systems have been proposed to provide immutable, independently verifiable chain-of-custody logs, potentially reducing disputes over evidence integrity by anchoring hash values and timestamps to a distributed, tamper-evident ledger rather than a single agency-controlled database. Pilot deployments by several national forensic laboratories suggest such systems can reduce the administrative burden of custody documentation, though questions remain about long-term key management and the legal weight courts will assign to blockchain timestamps relative to traditional notarization.

Memory and container forensics continue to evolve alongside virtualization and serverless computing architectures, where traditional disk-centric acquisition techniques are poorly suited to ephemeral compute instances that may exist for only seconds. Quantum-resistant cryptography is beginning to influence long-term evidentiary preservation strategies as current hashing and encryption schemes face eventual obsolescence, raising the practical question of how evidence hashed under an algorithm later deemed cryptographically broken should be re-authenticated for cases that remain pending or subject to appeal years after collection. Finally, the growing use of generative AI to fabricate synthetic media has spurred parallel research into forensic authentication techniques capable of distinguishing genuine recordings from convincing algorithmic fabrications, a capability that courts will likely require as a threshold matter before admitting audio or video evidence in contested cases

9. Recommendations

Based on the preceding analysis, the following measures are recommended to strengthen the alignment between digital forensic practice and legal requirements. First, jurisdictions should adopt internationally harmonized validation standards, such as ISO/IEC 27041 and 27042, accompanied by mandatory accreditation regimes for forensic laboratories and certification pathways for individual examiners, so that courts and counsel have an objective baseline against which to assess reliability claims. Second, expedited cross-border evidence-sharing mechanisms modeled on the CLOUD Act and the EU e-Evidence framework should be extended and reciprocally adopted more broadly, with judicial oversight retained at each stage to safeguard privacy interests and prevent circumvention of domestic protections through forum shopping.

Third, disclosure of methodology, training data provenance, and documented error rates should be made a mandatory precondition for admitting AI-assisted forensic findings, preserving the defendant's right to confront and meaningfully challenge the evidence against them. Fourth, specialized and recurring judicial and prosecutorial training on digital evidence should be institutionalized rather than left to occasional continuing-education seminars, given how quickly the underlying technology changes and how inconsistent admissibility standards are currently applied even within a single jurisdiction. Fifth, statutory clarity regarding encryption, lawful access mandates, and government hacking powers should be pursued through open legislative debate rather than ad hoc executive or judicial improvisation, calibrated to avoid undermining the broader cybersecurity ecosystem on which the reliability of digital evidence itself ultimately depends. Finally, sustained public investment in forensic laboratory capacity and workforce development is necessary to prevent evidence backlogs from becoming, in effect, a separate and unaddressed barrier to justice

10. Conclusion

Digital forensics and law are inextricably linked: forensic soundness is a precondition for legal relevance, while legal frameworks shape the boundaries within which forensic investigation may lawfully proceed. As digital ecosystems grow more complex through cloud computing, encryption, and artificial intelligence, the gap between technical capability and legal certainty risks widening unless deliberate efforts are made to harmonize standards, expedite cross-border cooperation, and equip legal practitioners with the technical literacy required to evaluate digital evidence critically. Sustained collaboration between technologists, legislators, and the judiciary remains essential to ensuring that justice systems can reliably respond to crime in the digital age without compromising fundamental rights.

Ethical Statement

*This study did not involve human participants, animals, or any intervention requiring ethical approval. Therefore, ethical approval was not required and is **Not Applicable**.*

Conflict of Interest

The author(s) declare that there is no conflict of interest regarding the publication of this manuscript.

Funding Statement

The author(s) received no financial support for the research, authorship, and/or publication of this manuscript.

Data Availability Statement

*No primary datasets were generated or analyzed during the current study. Therefore, data sharing is **Not Applicable**.*

Author Contribution Statement

All things been done by Author-1

Acknowledgements

The authors would like to express their sincere gratitude to Amity University for providing the academic environment and resources that supported the completion of this work.

Reference

[1] E. Casey, Digital Evidence and Computer Crime, 3rd ed. San Diego, CA, USA: Academic Press, 2011.

[2] National Institute of Standards and Technology, "Guide to

Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[3] ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, Geneva, Switzerland, 2012.

[4] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," Network Security, vol. 2011, no. 3, pp. 4-10, 2011.

[5] Council of Europe, "Convention on Cybercrime (Budapest Convention)," ETS No. 185, Budapest, Hungary, 2001.

[6] U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 2018.

[7] European Union, "Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters," Regulation (EU) 2023/1543.

[8] Computer Fraud and Abuse Act, 18 U.S.C. §1030 (United States).

[9] Computer Misuse Act 1990, c. 18 (United Kingdom).

[10] Police and Criminal Evidence Act 1984, c. 60 (United Kingdom).

[11] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Official Journal of the European Union, 2016.

[12] Information Technology Act, 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.

[13] Bharatiya Sakshya Adhiniyam, 2023 (India), s. 63.

[14] Stored Communications Act, 18 U.S.C. §2701-2712 (United States).

[15] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[16] ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories, International Organization for Standardization, Geneva, Switzerland, 2017.

[17] Riley v. California, 573 U.S. 373 (2014).

[18] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

[19] Microsoft Corp. v. United States, 584 U.S. ___ (2018) (per curiam, vacated as moot).

[20] R. v. Vu, 2013 SCC 60 (Canada).

[21] ISO/IEC 27041:2015, Guidance on assuring suitability and adequacy of incident investigative method, International Organization for Standardization, Geneva, Switzerland, 2015.

[22] ISO/IEC 27042:2015, Guidelines for the analysis and interpretation of digital evidence, International Organization for Standardization, Geneva, Switzerland, 2015.

[23] S. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64-S73, 2010.