

To analyze judicial approaches and evolving legal principles governing the admissibility and evidentiary value of digital evidence

Devendra Singh Rathore¹, Dr. Manju Koolwal^{2*}

¹Ph.D. Scholar, Nims School of Law, Nims University Rajasthan, Jaipur

²Professor, Department of Law, Nims School of Law, Nims University Rajasthan, Jaipur

***Corresponding Author:**

Dr. Manju Koolwal

Professor, Department of Law, Nims School of Law, Nims University Rajasthan, Jaipur

Email ID:- koolwalmanju212@gmail.com

Abstract:

N/A

INTRODUCTION

Cybercrime has emerged as a pressing challenge in the digital era, with online harassment and digital deception posing significant threats to personal security, dignity, and public trust in technology. The increasing sophistication of offenders, who exploit encrypted platforms, deepfake technology, and anonymization tools, has made the prosecution of such crimes heavily dependent on the credibility of forensic evidence. A critical dimension of this research focuses on bridging the gap between law and technology by aligning forensic innovations with judicial processes, thereby addressing evidentiary vulnerabilities that often lead to acquittals in cybercrime trials. Comparative insights are drawn from international practices, demonstrating the need for India to build resilient forensic systems capable of withstanding global standards of scrutiny. By fostering an integrated, technologically advanced, and legally robust approach, this study underscores that forensic science is not merely supportive but essential to delivering justice in cases of online harassment and deception, ultimately strengthening confidence in the digital justice system.¹

The study employs a mixed-methods research methodology, combining qualitative analyses of existing legal frameworks, academic literature, and case law with direct stakeholder engagement through structured questionnaires. Stakeholders include legal practitioners, forensic experts, law enforcement officials, policymakers, and academics, forming a global community united in the pursuit of justice. Their perspectives offer valuable insights into both the practical and theoretical dimensions of the challenges associated with digital and forensic evidence. Additionally, the research integrates interdisciplinary data from forensic science, cybersecurity, and legal studies to understand the topic comprehensively². A comparative analysis of international legal practices enhances the recommendations, ensuring they are relevant and adaptable globally.³ Key challenges in authenticating digital evidence include its susceptibility to tampering, maintaining an unbroken chain of custody, and possessing advanced technical expertise.⁴ These factors are crucial for ensuring the admissibility and reliability of evidence in court. Conversely, cybercrime prosecution faces obstacles such as jurisdictional disputes, the anonymity of perpetrators, and the inability of legal systems to keep pace with

rapidly evolving technologies. Furthermore, managing large volumes of digital evidence across multiple jurisdictions requires significant resources and, most importantly, international cooperation. This need for collaboration underscores the urgency and importance of our challenges.⁵

The identification phase, cybercrime investigators use many traditional investigative techniques (see: UNODC, Policing: Crime Investigation for a detailed analysis of these techniques), especially with respect to information and evidence gathering. For example, victims, witnesses, and suspects of a cybercrime are interviewed to gather information and evidence of the cybercrime under investigation (for guidance on interviewing suspects and adult and children witnesses and victims, see: UNODC, Anti-Human Trafficking Manual for Criminal Justice Practitioners, Module 9; UNODC, Toolkit to Combat Trafficking in Persons; UN Economic and Social Council (ECOSOC) Resolution 2005/20 Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime; UNODC, Justice in Matters involving Child Victims and Witnesses of

Crime; and Boyle and Vullierme, Council of Europe, A brief introduction to investigative interviewing: A practitioner's guide). Undercover law enforcement investigations have also been conducted to identify, investigate, and prosecute cybercriminals (examples of these investigations are included in Cybercrime Module 12 on Interpersonal Cybercrime and Cybercrime Module 13 on Cyber Organized Crime). Additionally, cybercrime investigators have conducted covert surveillance. This tactic is a "particularly intrusive method for collecting evidence. The use of covert surveillance measures involves a careful balancing of a suspect's right to privacy against the need to investigate serious criminality⁶

ResearchMethodology

This research is conducted using a doctrinal and analytical approach for qualitative research methodology. Domestic legislations, including the Bharatiya Sakshya Adhiniyam, 2023, Indian Evidence Act, 1872, and Information Technology Act, 2000, together with the relevant judicial precedents from the Supreme Court of India, constitute the major source of primary data analysis.⁷ In terms of comparative legal analysis, foreign statutory sources, which include the United States Federal Rules of Evidence (FRE) and the United Kingdom Police and Criminal Evidence Act, 1984 (PACE), are considered.

Secondary sources of data analysis include reports from the Law Commission of India, scholarly commentaries such as Law of Evidence by Sarkar, scholarly articles on forensic sciences and law, as well as digital forensics standards internationally (for instance, ISO/IEC 27037).⁸ The collected data is subject to critical legal analysis to discern any internal contradictions among statutory rules, any inconsistencies among judicial decisions, and friction between legal requirements and technical capacities for cyber forensics.⁹

ComparativeSynthesis

The following matrix synthesizes the structural divergence between the three jurisdictions:

Parameter	India (BSA, 2023)	United States (FRE)	United Kingdom (YJCEA / PACE)
Presumption of System Integrity	No assumption. System integrity must be actively demonstrated by the proponent through Section 63 certification.	Rebuttable presumption of reliability; verified by Rule 901's sufficiency standards.	Strong, rebuttable presumption. Unless proven otherwise, information is assumed to be reliable.
Certification Requirement	For all secondary digital evidence, Section 63 requires dual-signature certification (Part A & Part B).	Under Rules 902(13) and 902(14), self-authentication is optional; otherwise, oral testimony is used for authentication.	General principles of admission and hearsay apply; no statutory certification is necessary.
Expert Qualification Bottleneck	High. System administrators or government-notified cyber examiners must sign Part B in accordance with Section 79A of the IT Act.	Low. The Rule 902 certification can be signed by any qualified forensic examiner or IT specialist.	Low. Disputed technical matters are resolved via standard court-appointed or party-retained expert witnesses.
Operational Flexibility	Extremely rigid. Technical failures in certification can lead to absolute exclusion of critical evidence.	Highly flexible. Promotes judicial discretion and “gatekeeping” of reliability rather than hyper-technicality.	Prone to efficiency. Eliminates procedural bottlenecks, focusing trial time on substantive disputes of fact.

To analyze judicial approaches and evolving legal principles governing the admissibility and evidentiary value of digital evidence

To establish a solid academic baseline, the existing literature is categorized into three core thematic areas:

A. The Classic Regime of Section 65B of the Indian Evidence Act, 1872

The Certificate Debate: The early works concentrated on the statutory construction of Section 65B. Commentaries on the subject, such as Law of Evidence by Sarkar¹⁰, had argued whether secondary electronic evidence could be established without any certificate at all. Early legal opinion believed that Section 65B was a complete code itself, thereby completely supplanting any secondary evidence provisions.

Judicial Oscillations: The literature after State (NCT of Delhi) v. Navjot Sandhu¹¹ suggested that the relaxation of certification requirements undermined the authenticity of digital evidence since it permitted the oral evidence to be given without going through the technical procedure of verification. The later works have been critical of Anvar P.V.¹², since they suggest that the decision of Anvar P.V. takes a very technical approach, which resulted in ignoring the real evidences based on procedural lapses. Literature after Arjun Panditrao¹³ pointed out that it is impossible to get certificates from the adversarial third party.

B. Cyber Forensics, Chain of Custody, and Technical Vulnerabilities

Technical Volatility: The technical literature on digital forensics like Eoghan Casey's "Digital Evidence and Computer Crime"¹⁴ states that digital files are inherently volatile and highly prone to manipulation/deletion/alteration which can't be traced. Absence of SOPs at local police stations leads to compromising the integrity of the physical evidence during the act of search and seizure.

Grassroots Investigation Challenges in India: The delay in FSLs has been noted by forensic and police administration researchers for quite some time now. It is standard practice to use hardware write-blockers during imaging in the forensic process; but according to the literature emerging from within the country, grassroots-level investigative officers do not even have access to write-blockers, thus merely by booting up the seized mobile/computer.¹⁵

C. The Transition to Bharatiya Sakshya Adhiniyam, 2023

The Primary Evidence Loophole: New commentaries on the law with regards to the BSA raise a number of serious concerns about the possibility that evidence obtained via 'proper custody' be considered as primary evidence under Section 57(Explanation 5)¹⁶. Legal experts say that 'proper custody' can be highly subjective in police-controlled storage rooms (malkhanas), thereby posing the threat of admitting potentially compromised evidence devoid of the protection of a Section 63 certificate.

CONCLUSION

The development of India's digital evidence framework, which stretches from the IEA's nineteenth-century foundational work to the BSA's current structure, reveals a complicated interaction between procedural rules and computational realities. This study's central topic was whether the legal code, which is built on the ideas of a paper-based world, could adapt to the new digital landscape. Some crucial insights that show the persistence of past mistakes in the new code of laws have surfaced from the examination of historical changes to the legislative, judicial, and technical approaches to evidence in India.

The main finding of this study is that the original IEA, 1872's classical framework was fundamentally inappropriate for regulating the field of digital evidence. This is because Sir James Fitzjames Stephen's draft's central tenet, the Best Evidence Rule, was founded only on materialist presumptions.¹⁷ In the context of this nineteenth-century idea of architecture, a document was understood by its physicality rather than its contents, thus Section 62 simply needed the fabrication of the physical document as proof of contents.

When analog technologies were developed during the twentieth century, it became possible to assimilate magnetic tapes as documents by use of analogies where it was held in cases such as R.M. Malkani v. State of Maharashtra that impressions recorded on tapes magnetically were considered symbols made on a piece of paper.¹⁸ However, the advent of computer technology and digital information proved problematic to this model of proof, as unlike information recorded on analog media, which existed as physical inscriptions on tapes or filmstrips, digital computing information exists as a configuration of zeroes and ones across several different devices including local hard drives, synchronized cloud databases, and remote

servers.

Since the original database or server system was unlikely to be physically present in court and secondary evidence was unavailable due to intact systems, the viewing or accessing of digital files necessitates the process of replication rather than production, making the proof of contents via "primary evidence" practically impossible.¹⁹

The second key finding is that the Information Technology Act of 2000, which attempted to solve the issue by adding Sections 65A and 65B to the IEA²⁰, failed to establish a methodical approach to electronic evidence. Instead of creating rules for the acceptance of electronic evidence based on forensic computing principles, the law created a certification procedure that started a two-decade legal cycle..

REFERENCES

1. Gupta, A. (2021). Digital Evidence in India: A Judicial Perspective. *Indian Journal of Criminal Law*.
2. The Bharatiya Sakshya Adhiniyam, 2023.
3. Information Technology Act, 2000.
4. Lars Daniel, Digital Forensics—What Exactly Is Digital Evidence?, Retrieved from
5. Sharma, V., & Reddy, P. (2020). Cyber Crime and Digital Evidence: Challenges in Prosecution. *Law .Review Journal*.
6. P.C. Sarkar and M.C. Sarkar, *Law of Evidence* 1240 (LexisNexis, New Delhi, 15th edn., 2020).
7. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
8. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, *supra* note 4.
9. Eoghan Casey, *Digital Evidence and Computer Crime* 89 (Academic Press, London, 3rd edn., 2011).
10. G.S. Bajpai, "Scientific Investigation in Indian Criminal Justice: A Ground Reality Check" 12 *Indian Journal of Criminology* 45 (2021).
11. S.S. Prasad, "Deciphering the Digital Trial: Challenges under Bharatiya Sakshya Adhiniyam" 66 *Journal of the Indian Law Institute* 45 (2024).
12. hikhar Goel, 'Paper in the Age of the Digital: The Curious Case of 65-B Certificates in India' 11 *Asian Journal of Law and Society* 435 (2024).
13. The Indian Evidence Act, 1872 (Act 1 of 1872), s. 65B(4).
14. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
15. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
16. Parliamentary Standing Committee on Home Affairs, *Three Hundred and Eightieth Report on the Bharatiya Sakshya Bill, 2023* (Rajya Sabha Secretariat, New Delhi, 2023).
17. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(d).
18. *Ibid*, s. 2(1)(t).
19. Sir James Fitzjames Stephen, *The Indian Evidence Act, 1872* (Thacker, Spink & Co., Calcutta, 1872)
- 12.
20. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 2(1)(t).