Digital Evidence and Due Process: Challenges in Balancing Technology and Fair Trial Rights in India

Akshita Goswami
Assistant Professor, Department of Management, Jagannath University, Bahadurgarh, Jhajjar (Haryana)

Abstract With the rise of digital technologies, Indian courts increasingly rely on digital evidence—including surveillance footage, metadata, and digital communications—during criminal trials. Although this technological shift enhances investigation and adjudication, it raises significant concerns about due process, privacy, and the right to a fair trial. This paper examines how Indian law accommodates digital evidence under the Indian Evidence Act, 1872, highlights the procedural and technological challenges surrounding its admissibility, and evaluates the due process implications. Drawing on doctrinal research and comparative insights, the study proposes legal and policy reforms to strengthen the legitimacy and reliability of digital evidence within India's criminal justice framework.

Keywords: Digital Evidence, Due Process, Fair Trial, Indian Evidence Act, Admissibility, Criminology, Privacy

1. Introduction

Technological advancements have drastically altered the legal framework of criminal litigation in India. The growing prevalence of digital footprints—such as call records, internet activity logs, and social media interactions—has transformed how evidence is collected and presented in courts. While this enhances prosecutorial efficiency, it simultaneously presents a host of legal and ethical dilemmas concerning admissibility, privacy, and the right to a fair trial. In this context, ensuring that digital evidence meets legal standards while upholding constitutional safeguards becomes paramount.

2. Objectives of the Study

- To trace the evolution of legal norms concerning digital evidence in India.
- To identify procedural and technological challenges related to the admissibility of digital records.
- To assess the impact of digital evidence on constitutional guarantees of due process and fair trial.
- To compare India's legal practices with global standards in digital evidence handling.
- To propose legal and institutional reforms to ensure evidence integrity and accountability.

3. Methodology

This study adopts a qualitative and doctrinal methodology. It analyzes primary sources such as statutes (e.g., the Indian Evidence Act and Information Technology Act), constitutional provisions, and judicial decisions. Secondary sources include academic journal articles, international standards, legal reports, and case studies. The research also incorporates comparative legal analysis to contrast Indian legal practices with those in jurisdictions like the United States, United Kingdom, and European Union.

4. Literature Review

Sharma (2021) explores interpretational inconsistencies in Indian trial courts regarding Section 65B of the Indian Evidence Act, which governs electronic evidence. Saini (2022) discusses the manipulation of digital records and emphasizes the need for integrity protocols. Comparative scholars like Chander and Sunstein (2020) analyze how digitalization and algorithms challenge traditional evidence law. Prasad (2019) argues that India's forensic ecosystem lacks the institutional capacity to preserve and verify digital data reliably. The European Union Agency for Cybersecurity (ENISA, 2023) advocates for blockchain and cryptographic hashing to maintain data integrity.

5. Legal Framework in India

The Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000, governs the admissibility of electronic records. Section 65A and 65B specifically deal with the evidentiary requirements of digital documents. Section 65B mandates that a certificate of authenticity be produced along with any electronic record. This certificate must identify the device used, describe the process by which the record was produced, and be signed by a responsible official.

Judicial developments:

- *State (NCT of Delhi) v. Navjot Sandhu* (2005) allowed secondary evidence even without a certificate under Section 65B.
- *Anvar P.V. v. P.K. Basheer* (2014) overruled the Navjot Sandhu ruling, making the certificate mandatory.
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) clarified that such certificates are required unless the evidence originates from the device owner.

Despite the clarity in higher court rulings, procedural irregularities in trial courts continue to create legal uncertainty.

6. Challenges in Admissibility and Use of Digital Evidence

6.1 Procedural Ambiguities

In practice, many investigative agencies and trial courts struggle with procedural compliance under Section 65B. The lack of uniform protocols and technical knowledge leads to inconsistent application of evidentiary rules.

6.2 Risk of Tampering and Forgery

Digital content can be easily altered or fabricated. Without forensic verification mechanisms such as cryptographic hashing, the authenticity of screenshots, videos, and metadata can be called into question.

6.3 Lack of Standard Protocols

India does not yet have comprehensive statutory or regulatory standards for digital evidence management. In contrast, countries like the U.S. and U.K. have codified chain-of-custody procedures, forensic lab certifications, and audit trail requirements.

7. Due Process and the Right to a Fair Trial

The Constitution of India guarantees due process under Article 21. As held in *Maneka Gandhi v. Union of India* (1978), any legal procedure must be fair, just, and reasonable. Improperly obtained or unverified digital evidence may violate:

- The right to cross-examine witnesses
- The presumption of innocence
- The right against self-incrimination

Post-*Justice K.S. Puttaswamy v. Union of India* (2017), privacy has been recognized as a fundamental right. Evidence obtained via unauthorized surveillance tools—such as Pegasus spyware—raises serious constitutional concerns.

8. Comparative Legal Analysis

Country	Framework	Safeguards
USA	Federal Rules of Evidence Rule 902(14)	Chain of custody, hash verification
UK	Police and Criminal Evidence Act (PACE)	Digital imaging standards, audit trails
EU	GDPR, ENISA Guidelines	Cyber-forensic protocols, blockchain
India	Evidence Act, IT Act	Certificate under Section 65B

India trails its global counterparts in developing centralized and verifiable systems for digital evidence authentication.

9. Case Studies

9.1 Bhima Koregaon Case

International forensic audits revealed malware-based planting of documents on the accused's computers. The case exposed the risk of manipulated evidence and the absence of independent forensic validation.

9.2 Aarushi-Hemraj Case

Inconsistent reliance on digital records such as call logs and internet activity led to conflicting judicial interpretations, underscoring the importance of interpretive clarity and evidentiary standards.

9.3 Pegasus Spyware Allegations

Reports of state-sponsored surveillance using Pegasus spyware sparked legal debates around the admissibility and ethicality of evidence obtained through unauthorized digital surveillance.

10. Recommendations

1. **Enact a Digital Evidence Management Law**: Establish legally binding standards for evidence acquisition, verification, and retention.
2. **Implement Forensic Hashing and Blockchain**: Secure electronic records using cryptographic tools to ensure authenticity.
3. **Create a Central Digital Evidence Registry**: Facilitate cross-jurisdictional access and maintain a verified chain of custody.
4. **Mandatory Technical Training**: Equip judges, lawyers, and investigators with technical knowledge through continuous professional education.
5. **Ensure Digital Legal Aid**: Guarantee access to digital forensics and technical counsel for the defense, especially for underrepresented groups.

11. Conclusion

While digital evidence plays a pivotal role in modern legal proceedings, its misuse or mishandling can undermine constitutional guarantees. Legal reform, combined with technological safeguards and institutional accountability, is necessary to preserve the integrity of India's criminal justice system. Harmonizing evidentiary innovation with due process principles is essential to achieving procedural fairness.

References

2. Chander, A., & Sunstein, C. R. (2020). Evidence law in the age of algorithms. *Harvard Journal of Law & Technology, 33*(2), 201–245.
3. ENISA. (2023). *Cybersecurity for digital evidence*. https://www.enisa.europa.eu
4. Prasad, V. (2019). Digital forensics and legal gaps. *Law & Tech Journal, 7*(1), 55–69.
5. Saini, A. (2022). Fair trial in the digital age. *Indian Bar Journal, 28*(3), 101–120.
6. Sharma, R. (2021). Admissibility of digital evidence in India. *NLUJ Law Review, 13*(2), 45–62.
7. U.S. Federal Rules of Evidence, Rule 902(14). (2017).
8. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
9. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
10. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
11. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.