

# Deepfakes and Due Process: Rethinking Authenticity of Social Media Evidence in India's New Digital Evidence Regime

G. Sona <sup>a</sup>, Y. Mahalingam <sup>b</sup>

<sup>a</sup> Department of Law, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.

E-mail: sg4312@srmist.edu.in

<sup>b</sup> Assistant Professor, Department of Law, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India. E-mail: mahalinv@srmist.edu.in

---

## Abstract

The use of social media has become the central point of criminal investigation and trial, providing real time data of behavior, communication, and the location of suspects on WhatsApp, Instagram, and X platforms. However, such material is only accepted by courts when it meets great requirements of relevance, authenticity, integrity and legal collection as per international rules of digital evidence (23711). This theoretical and comparative research examines the transformation of the Indian regime since the Indian Evidence Act, 1872, and IT Act, 2000 (Sections 65A-65B) to Bharatiya Sakshya Adhiniyam, 2023 which balances electronic records with traditional documents whilst maintaining an intensive and metadata intensive certifications procedure under Section 63 (51018). Using the international literature on social media forensics, metadata-based authentication of digital evidence, and deepfakes, the research identifies core admissibility requirements and compares the practice in India with the international practice (23471416). It recognizes the main issues, such as manipulation and AI generated deepfakes, lapses in the procedure, cross border access to data, insufficient forensic capabilities and judicial skills (135131619). The article explains that the new framework in India is mostly convergent with the best practice in the international world but will be weak without standardization of forensic procedures, platform-specific applications, international partnership, and systematic training of investigators and courts (235716). It ends by suggesting improvements to enhance authenticity checks, chain of custody documentations, and privacy controls to enable the utilization of social media evidence without derailing the rights to fair trials.

**Keywords:** Social Media Evidence, Admissibility, Indian Legal Systems, Digital Forensics, Deepfakes and Chain of Custody.

---

## Introduction

In criminal cases, evidence in social media has become unavoidable, however, it can only be admitted to the court when conditions of authenticity, integrity, relevance, and collection are fulfilled strictly as required under 2. The evidence of social media has revolutionized criminal investigation and criminal trials across the globe by providing information on real-time behavior of suspects, alibi, and communication. WhatsApp, Instagram, and X are the platforms that allow prosecutors to access posts, chats, and metadata that are connected to offenses directly, but it is high volatility, and it has to be strongly validated. Courts all over the world do not admit informal screenshots, but they demand forensic-extracted ones to avoid the possibility of manipulation by editing programs and deepfakes.

This evidentiary change in India is accompanied by a modernizing legislative change in the form of the Bharatiya Sakshya Adhiniyam 2023, which is a rejection of old certification obstacles in Sections 65A-65B. The paper bridges the void in forensic capacity and cross-border access to a data, and suggests uniform guidelines on how the probative ability of social media can be utilized without affecting fairness (Arshad et al., 2025). The further parts of 2 identify legal frameworks, admissibility tests, challenges, and future trends (Rakha, 2024).

## Literature Review

Section 2 of this literature review presents a discussion on the contextual challenges of the topic of social media evidence in a criminal trial, with the framework of legal admissibility discussed in a global context with an Indian orientation. It summarizes the academic literature and legal cases to define the evolution, fundamental needs, obstacles, and tendencies that impact the work with digital evidence (Angel et al., 2024). The discussion relies on the agreement of such sources as Consensus app papers, pointing out the alignment towards standards in the face of technological disruptions.

### Contextual Issues

#### Legal Admissibility Framework (India in Global Context)

- In many jurisdictions, social media evidence (as well as any other digital evidence) is admissible when it is relevant, authentic, reliable, and obtained lawfully 21820.
- In India, admissibility changed under Indian Evidence Act, 1872 and IT Act, 2000 into rules of specific of electronic records in Section 65A-65B with certification as a significant requirement 78.
- The rulings of the courts below 65B prohibited admission of secondary electronic records without an appropriate certificate, creating a doctrinal dispute and subsequently permitting in rare cases 8.
- The modernization of this regime is the Bharatiya Sakshya Adhiniyam 2023:
  - Treats e records as equal to traditional documents and rejects them simply because they are electronic 14 (Malik, 2024).
  - Makes a standardized process of certification (Section 63 BSA) which courts are already implementing with strictness, e.g. refusal of the evidence of WhatsApp/email without appropriate certification and metadata corroboration 14.

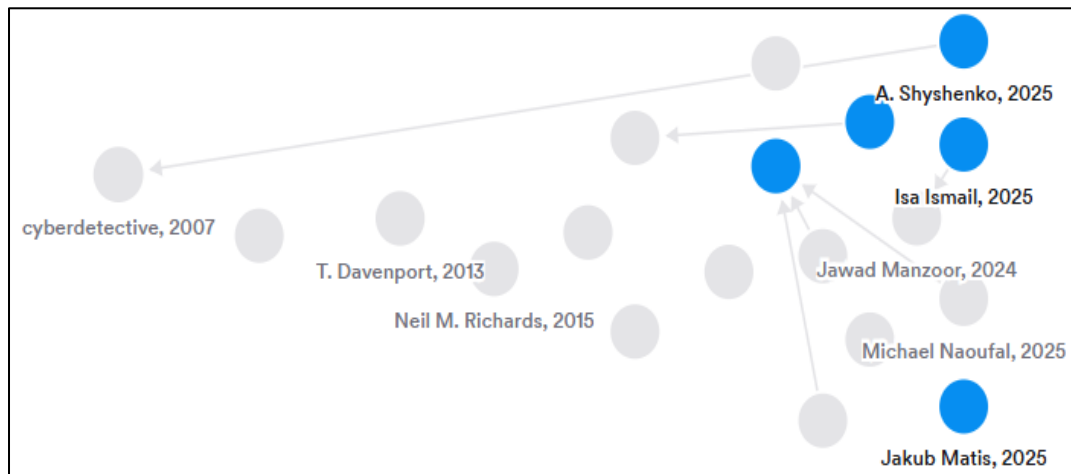


**Fig. 1: Literature Case Graph**

Fig. 1 is a case study of literature that shows the connection and publishing timeline of many writers, with a focus on cyber detective and influential figure research from 2007 to 2025.

### **BSA 2023 Streamlines Prior Rigidities While Upholding Safeguards**

- The Evidence Act of 1872, which was amended through the IT Act 2000, required certificates on secondary copies in sections 65A-65B, and certain judges, such as Anvar P.V. v. P.K. Basheer (2014), interpreted this literally.
- Following Arjun Panditrao Khotkar (2020), courts permitted exceptions of primary evidence/ oral evidence where certification gaps existed to permit admissibility without the diminution of scrutiny.
- Section 63 of the BSA certifies uniformity in e-records and stipulates information such as device specifications and hash validation, which have been used in recent cases to dismiss uncertified chats.
- BSA under Subsection 2(1)(d) proposes e-evidence as being mathematically equivalent to paper documents and this does not exclude any category of evidence based on its form, which encourages effectiveness when trial is conducted in cyberspace.

### **The Structure of India is Not Robust but Rather Compliant with the International Standards with the Specific Certification Requirements by the BSA 2023**

- Digital evidence, such as postings on social media, is necessary due to global consistency, which means that they need to show probative value in connection with facts of the case, such as the establishment of intent by use of timestamps or geolocation information.
- Authentication is frequently used to check the integrity of metadata, such as hash values and device logs, which prevents the difficulty in counterfeit content, such as the case of deepfakes.
- The issue of reliability depends on chain-of-custody guidelines, meaning the tamper evident treatment of the data during extraction to presentation which is one of the points stressed in the cross-jurisdictional guidelines.
- Legal acquisition requires adherence to privacy regulations, including warrants to request platform data, a trade-off between the evidences and the rights within the frameworks such as GDPR equivalents.

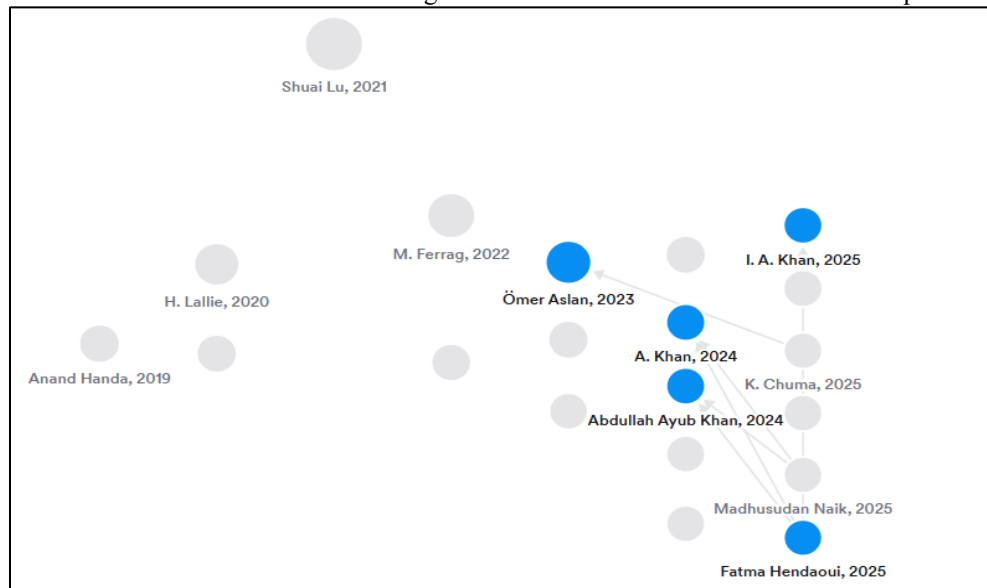


**Fig. 2: Literature Review Graph**

Fig. 2 is a case study of the literature that shows the relationships and publication dates of the leading researchers. It focuses on works produced between 2019 and 2025, with a considerable amount of output in 2024 and 2025.

### **Core Admissibility Requirements for Social Media Evidence**

Essential criteria for social media admissibility as laid out in table 1 include authenticity, relevance, standard content procedures, reference requirements, and publishing, among other things.

**Table 1: Core Legal Tests for Social Media Admissibility**

| Requirement                  | Typical Content / Practice                                                                        | Citations  |
|------------------------------|---------------------------------------------------------------------------------------------------|------------|
| Relevance                    | Links posts/chats/metadata to facts in issue (presence, intent, association)                      | 2318       |
| Authentication               | Metadata, hash values, device examination, corroborative testimony to prove authorship and origin | 237141820  |
| Integrity & Chain of Custody | Forensic imaging, logs of access, tamper-evident storage, expert validation                       | 23141820   |
| Lawful Collection & Privacy  | Warrants/subpoenas; compliance with data-protection and platform rules; no arbitrary intrusion    | 2411121820 |

### The Major Obstacles of Criminal Trials

- **Authenticity & Deepfakes:** Both courts and researchers emphasize the ease of manipulation, particularly of images, video, and artificial intelligence-based content and require expert forensics and metadata analysis 5111418.
- **Procedural Gaps and Inconsistency:** There are numerous systems (Indonesia, Tanzania, Ukraine, Slovakia) that do not have elaborate procedural codes on digital evidence, which result in unclear standards, and divergent judicial practice 15619.
- **Issues Platform and Cross Border Issues:** Data located in foreign countries and platform takedowns make social media content difficult to preserve and obtain lawfully in a timely manner 2411121314.
- **Capacity Deficits:** Courts and investigators might not have a digital forensic knowledge base and infrastructure, undermine the probative value and subject them to the risk of being excluded as otherwise useful material 1314181920.

### Emerging Trends (2024-2026 and beyond)

- **Stricter but Pro digital Courts:** Courts are beginning to accept the importance of digital evidence, but this will only come with very strict chain of custody and certification and not informal screenshots 137141820.
- **New Indian Codes (BNS, BNSS, BSA 2023):** These changes are designed to simplify the process of cybercrime investigation and handling of digital evidence, but they also bring up the issue of privacy, surveillance, and forensic capacity 471415.
- **Platform Specific Forensics:** The increasing amount of literature on Instagram and other platforms focuses on the use of special tools to restore deleted information, work with metadata, and enable court admissibility 213.
- **International Harmonization:** Comparative research findings demonstrate the point of convergence between the standards of reliability, documentation, and rights protection, and demand a set of uniform guidelines and training 51115181920.

### Purpose of this Study

- In order to investigate the admissibility standards of social media evidence in criminal proceedings, one would need to pay attention to the concept of authenticity, integrity, relevance, and legality of collection.
- To follow the legal development of India since the Indian Evidence, Act 1872 and IT Act 2000(Sections 65A-65B) to the Bharatiya Sakshya Adhiniyam 2023 (BSA).
- In order to match the Indian standards to international practices, the emphasis should be put on the consistency of the requirements such as metadata verification and chain-of-custody.
- To find the main issues like deepfakes, lapses in the procedure, international access to data, and insufficiency of the forensic capacity.
- To examine the new trends, such as more stringent certification based on BSA Section 63, platform-specific forensics and international harmonization.
- To comment about implications on investigations, privacy protection and why judicial training and infrastructure upgrades are required.

### Research Methodology

This paper uses a qualitative, doctrinal, and socio-legal approach to research, focusing on normative legal research on law and case law as well as analytical synthesis of technical deepfake forensics literature with Indian standards of evidence. A discretionary empirical element will include semi-structured interview or survey of purposive judges,

prosecutors, defense attorneys, cyber-crime investigators, and forensic specialists in order to record the view of deepfakes menaces, authentication measures as well as dependence on AI detection devices.

### **Doctrinal Analysis**

The doctrinal part reviews the main Indian legal texts, such as a clause on electronic evidence and authenticity under the Bharatiya Sakshya Adhiniyam 2023, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, IT act 2000, and data protection standards and applicable offenses of fabricating, obscenity, impersonation, and fraud. It even examines Supreme Court and High Court cases on the admissibility of electronic evidence under the previous Section 65B regime, video/audio authenticity, expert evidence, and chain-of-custody provisions, in the absence of deepfake specific cases. A comparative analysis puts them up against the international media forensics standards of deepfake detection instruments and responses in foreign jurisdiction and finds gaps in reliability and admissibility (Azad, 2026).

### **Technical Review**

The technical part performs a narrative/systematic review of the deepfake detection techniques, including GAN-based forensics, multimodal analysis, active/passive authentication, and chain-of-custody issues. It correlates such ideas as model reliability, interpretability, robustness, and real-world performance with the Indian standards of expert evidence and the beyond reasonable doubt standard.

### **Empirical and Integrative Approach**

The socio-legal component codes the interviews with stakeholders thematically to demonstrate inconsistencies among legal framework, technical capabilities and courtroom realities, such as perceptions of deepfakes, existing video/social media verification, and the issue of AI tool bias. The analysis of data is a combination of interpretive doctrinal comparisons and technical syntheses of detection limits (e.g. cross-modality problems, dataset bias, adversarial attacks), and points to due-process risks, such as false convictions. The paper ends with a recommendation of the structure of the evidentiary standards on reports detecting deepfakes, such as procedural safeguarding, model disclosure, and certification measures (Abdullah et al., 2025).

### **Research Overview**

The paper addresses background of the role of social media evidence, legal principles (e.g. Section 65A-65B, Section 63 BSA), fundamental admissibility criteria (relevance, authentication using metadata/hashes, integrity using chain of custody, legally gathered), obstacles (problems with authenticity, issues with capacity), and trends (tougher courts, platform forensics, international harmonization). It also has a table of requirements and covers Indian evolution of strict certification to modernization.

### **Implications**

#### ➤ **Better Evidentiary Value, but with Severe Protection**

The change of Section 65B to the Bharatiya Sakshya Adhiniyam (BSA) in India increases the admissibility and status of electronic records, such as that of social media, as primary evidence, under the condition that authenticity, chain of custody and certification are sufficiently established 6314.

#### ➤ **Requirement of a Strong Digital Forensics and Standards**

There is actual danger of manipulation by courts and investigators, particularly deepfakes; according to jurisprudence by the Supreme Court, recent BSA specialized scholarship emphasizes that electronic evidence may hinder justice without non-technical verification and maintenance 361. This requires industry standard forensic procedures, hash integrity and specialist-based certification systems 1417.

#### ➤ **Capacity Building and Gaps in Infrastructure**

Cybercrime and forensics in India Studies have also pointed out poor laboratory capacity, lack of standard procedures and training to create inadmissibility, delays or erroneous results 11711. There is a strong necessity of continuous judicial and investigational training because AI driven fakes are spreading 8 (Singh et al., 2025).

#### ➤ **Cross Border Data, Privacy and Due Process**

The increasing digital evidence strength increases privacy and Article 21 anxieties; the trade-off between security and fundamental rights has consistently been found as a central issue 1514. The cross-border access of data and cloud evidence are still bottlenecks, which complicate access to social media platforms on time 1519.

## Discussion and Conclusion

The recent digital evidence system in India has made social media and AI-manipulated material become the core of inquiry and decision making, particularly following the move to the new digital evidence system in India namely the Bharatiya Sakshya Adhiniyam (BSA) as a replacement of the old Section 65B certificate system. The BSA makes electronic records primary evidence and requires uniform certification and authenticity standards but successful application of the increased evidentiary authority requires strict compliance with authenticity, reliable certification, and a continuous chain of custody with digital forensics and always-on training of investigators, prosecutors, and judges.

A discussion thus focuses on maximizing the probative usefulness of social media evidence using strict technical and procedural criteria hashing of evidence, metadata, documented chain-of-custody of evidence, and expert validation and reducing the uncertainties of privacy invasion, evidence mishandling, and unfair prejudice. Cross-jurisdictional admissibility Research around the world has indicated that there is continued lack of a consistency in legal standards on digital evidence, cross-jurisdictional cooperation among providers, and that this is creating barriers of a significant nature to accessing data across-borders in cases of cybercrime and that the reliance on evidence taken in one jurisdiction to be used in another is uncertain. The same would be the case in South Asian systems, where poor chain-of-custody practices and ambiguous cross-border practices often bring credibility and fairness in cybercrime prosecutions.

In this atmosphere, the new criminal legislation (BNS, BNSS, BSA) in India can be characterized as a major point in criminal law reform: it simplifies the gathering and admissibility of digital evidence and is more responsive to AI-driven and cyber-enabled crimes, but the lack of forensic infrastructure, technical capacity, and privacy protection as perceived may pose a threat to due process when left unaddressed (Bharti & Gupta, 2025). This regime will have to be constitutionalized with the procedures and privacy safeguards that are clear, capacity-building in courts and investigative agencies, and more predictable and rights-respectful mechanisms of access across borders to be implemented. With high thresholds of authenticity, certification, and chain-of-custody, and state investment in the capacity and training in forensic evidence, India can use social media evidence and combat deep fake-driven cybercrime without sacrificing due process and basic rights under Articles 20 (3) and 21.

## References

- Arshad, M., Ahmad, A., Onn, C. W., & Sam, E. A. (2025). Investigating methods for forensic analysis of social media data to support criminal investigations. *Frontiers in Computer Science*, 7, 1566513. <https://doi.org/10.3389/fcomp.2025.1566513>
- Azad, M. D. (2026, March 5). Admissibility of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023: A critical analysis. *Indian Journal of Law and Legal Research*. <https://www.ijlrr.com/post/admissibility-of-electronic-evidence-under-the-bharatiya-sakshya-adhiniyam-2023-a-critical-analysis>
- Angel, O. M., Mercedes, C. F. Y. M., Elisa, Q. A., Joaquin, D. P. J., Giovanna, C. D. O. D. D., & Beatriz, G. Q. (2024). Digital evidence as a means of proof in criminal proceedings. *Revista de Gestão Social e Ambiental*, 18(4), e04585-e04585.
- Bharti, N., & Gupta, N. (2025). Admissibility of Electronic Evidence in India: Legal Framework, Judicial Trends, and the Impact of the Bharatiya Sakshya Sanhita, 2023. *International Journal for Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2025.v07i04.54750>
- Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. *Research Journal for Social Affairs*, 3(5), 795-805. <https://doi.org/10.71317/RJSA.003.05.0375>
- Malik, N. (2024). Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings as per Bhartiya Sakshya Adhiniyam, 2023. *Universal Research Reports*, 11(4), 64-72. <https://doi.org/10.36676/urr.v11.i4.1311>
- Rakha, N. A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2), 23-54. <https://doi.org/10.22201/ij.24485306e.2024.2.18892>
- Singh, V., Jindal, B., Saini, V., Ranga, P., Rani, R., Gupta, H., & Banger, M. (2025). Impact of e-records as evidence in the judicial system under the Bharatiya Sakshya Adhiniyam 2023. *Metallurgical and Materials Engineering*, 31(3), 340–345. <https://doi.org/10.63278/1383>