International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 05-04-2025, Accepted: 06-05-2025, Published: 22-05-2025
Volume 7, Issue 2, 2025, Page No. 201-207

AI-generated identity theft detection and digital evidence: challenges for Indian courts

Sakshi Gupta[1], Dr. Bhavna Singh[2]
[1] Research Scholar, Department of legal studies, Banasthali vidyapith, Rajasthan, India
[2] Assistant Professor Department of legal studies, Banasthali University, Jaipur, Rajasthan, India
DOI: https://doi.org/10.66856/ijlpsr.2025.7.2.8144

Abstract
The rapid advancement of generative artificial intelligence (AI), particularly deep learning, large language models, voice-cloning systems, and deepfake technologies, has transformed both digital innovation and cybercrime. AI-generated identity theft has emerged as one of the most sophisticated forms of cyber-enabled criminality, allowing offenders to fabricate realistic digital identities, impersonate individuals, manipulate biometric characteristics, and generate highly convincing synthetic evidence. These developments present unprecedented challenges for criminal investigations, digital forensic science, and judicial determination of authenticity. The Indian legal framework, despite significant reforms through the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), and the Digital Personal Data Protection Act, 2023, remains largely designed for conventional electronic evidence rather than AI-generated synthetic media.

This paper critically analyses the emerging legal and evidentiary challenges associated with AI-generated identity theft before Indian courts. Using a doctrinal legal research methodology supported by comparative legal analysis, the study evaluates the adequacy of Indian statutory provisions governing digital evidence, forensic authentication, identity-related cyber offences, and judicial treatment of AI-generated content. Comparative references are drawn from the European Union Artificial Intelligence Act, 2024, selected United States legislative initiatives, and international forensic standards to identify best practices applicable within the Indian legal system.

The study finds that the existing evidentiary framework continues to rely heavily upon certificate-based authentication mechanisms that are inadequate for detecting sophisticated AI-generated manipulation. The absence of specialised forensic infrastructure, judicial protocols for evaluating AI-generated evidence, and dedicated statutory provisions governing synthetic identities significantly weakens India's preparedness against emerging cyber threats. The paper argues for a comprehensive legal response combining legislative reform, AI-specific evidentiary standards, institutional capacity-building, judicial education, forensic innovation, and international regulatory cooperation. Such reforms are essential to preserve the integrity of digital evidence, protect constitutional rights, and strengthen public confidence in the administration of justice in the era of artificial intelligence.

Keywords: Artificial intelligence, identity theft, digital evidence, deepfakes, Bharatiya Sakshya Adhiniyam, 2023, cyber crime, digital forensics, Indian courts

Introduction

Artificial Intelligence (AI) has emerged as one of the defining technologies of the twenty-first century, fundamentally reshaping economic activity, governance, healthcare, education, communication, and criminal justice. Recent advances in generative artificial intelligence including transformer-based large language models, Generative Adversarial Networks (GANs), diffusion models, and sophisticated voice-cloning systems have dramatically enhanced the ability of machines to create realistic text, images, videos, and audio recordings that closely resemble authentic human-generated content. While these innovations have produced substantial societal and economic benefits, they have simultaneously transformed the landscape of cybercrime by enabling highly sophisticated forms of deception, impersonation, and identity theft.

Unlike traditional cyber offences that generally relied upon stolen passwords, phishing attacks, or database breaches, AI-generated identity theft exploits synthetic media capable of reproducing an individual's voice, facial expressions, biometric characteristics, handwriting, and behavioural patterns with remarkable accuracy. Criminals may therefore fabricate convincing digital identities without physically accessing the victim's credentials or biometric information. Such capabilities have significantly expanded opportunities for financial fraud, cyber extortion, online harassment, electoral misinformation, corporate espionage, and judicial deception.

The emergence of deepfake technology illustrates the magnitude of this transformation. Deepfakes are AI-generated synthetic audio or visual recordings that realistically depict individuals saying or doing things that never occurred. Modern deepfake systems can produce facial movements, speech patterns, emotional expressions, and lip synchronisation that are often indistinguishable from authentic recordings. Consequently, digital photographs, surveillance footage, audio recordings, and video evidence once regarded as highly reliable forms of evidence can no longer be presumed authentic without sophisticated forensic verification.

India presents a particularly significant context for examining these developments because of its rapidly expanding digital ecosystem. Government initiatives such as Digital India, Aadhaar-based digital identity systems, Unified Payments Interface (UPI), DigiLocker, electronic

governance platforms, and widespread smartphone penetration have accelerated digital transformation across both public and private sectors. While these initiatives have enhanced accessibility and economic inclusion, they have simultaneously increased dependence upon electronic identities and digital authentication mechanisms. As digital transactions become increasingly integrated into everyday life, AI-generated identity theft poses substantial risks to financial security, privacy, public trust, and national cybersecurity.

The existing Indian legal framework governing identity theft principally derives from Sections 66C and 66D of the Information Technology Act, 2000[6], alongside corresponding offences codified under the Bharatiya Nyaya Sanhita, 2023 [2]. Similarly, electronic evidence is presently regulated under the Bharatiya Sakshya Adhiniyam, 2023 [3], which substantially replaces the earlier provisions contained in the Indian Evidence Act, 1872. Although these legislative reforms modernise several procedural aspects concerning digital evidence, they remain largely premised upon conventional electronic records rather than AI-generated synthetic content capable of sophisticated manipulation. The evidentiary assumptions underlying certificate-based authentication were formulated during an era when electronic records generally originated from identifiable computer systems operated by identifiable custodians. Generative AI fundamentally disrupts these assumptions by producing synthetic content through distributed computational systems that frequently operate across multiple jurisdictions and anonymous infrastructures.

The challenges confronting Indian courts extend beyond statutory interpretation. Judicial institutions increasingly encounter electronic evidence whose authenticity cannot be reliably established through traditional evidentiary methods alone. Digital forensic laboratories similarly face significant technical limitations in detecting increasingly sophisticated synthetic media generated by rapidly evolving AI models. Investigating agencies often lack specialised expertise required to identify AI-generated manipulation during criminal investigations, while judges must evaluate expert testimony concerning technologies that remain scientifically dynamic and technically complex. Consequently, courts must determine not only whether electronic evidence satisfies statutory admissibility requirements but also whether the underlying digital content genuinely represents historical reality.

International developments further illustrate the urgency of these concerns. The European Union Artificial Intelligence Act, 2024[34] introduces comprehensive transparency obligations requiring disclosure of AI-generated content and establishes regulatory safeguards for high-risk AI systems. Similarly, numerous jurisdictions, including several states within the United States, have enacted legislation specifically addressing deepfake technologies, election interference, synthetic media, and biometric impersonation. These comparative developments demonstrate an emerging international consensus that conventional cybercrime legislation alone cannot adequately regulate AI-generated identity fraud.

Against this background, the present research critically examines the legal, forensic, and evidentiary implications of AI-generated identity theft within the Indian criminal justice system. The study seeks to answer the following central research question:

To what extent does the existing Indian legal framework adequately address the challenges posed by AI-generated identity theft and digital evidence, and what reforms are necessary to strengthen judicial responses in the age of generative artificial intelligence?

The study pursues four principal objectives. First, it analyses the existing statutory framework governing AI-enabled identity theft and electronic evidence under Indian law. Second, it evaluates the evidentiary challenges associated with authentication, admissibility, and forensic verification of AI-generated digital content before Indian courts. Third, it compares India's regulatory approach with contemporary international developments, particularly the European Union Artificial Intelligence Act and selected United States initiatives. Finally, it proposes legislative, institutional, and judicial reforms designed to enhance India's capacity to address emerging challenges associated with generative artificial intelligence.

The paper is organised into five substantive parts. Following this introduction, Part II critically reviews the existing literature concerning AI-generated identity theft, digital forensics, and evidentiary regulation of electronic records. Part III explains the doctrinal methodology employed for analysing statutory provisions, judicial decisions, and comparative legal frameworks. Part IV presents the principal findings through thematic discussion concerning statutory inadequacies, evidentiary authentication, forensic infrastructure, comparative regulatory models, and judicial developments. Finally, Part V concludes by summarising the principal findings, recommending comprehensive legal reforms, and identifying future directions for research concerning artificial intelligence and digital justice.

Literature Review

The scholarly discourse on artificial intelligence (AI), identity theft, and digital evidence has expanded significantly over the past decade, driven by rapid technological developments and the increasing sophistication of cyber-enabled crimes. Nevertheless, the intersection of AI-generated identity theft and evidentiary law remains an emerging area of legal scholarship, particularly within the Indian context. Existing literature may broadly be categorised into four interconnected themes: (i) AI-generated identity theft and cybercrime; (ii) digital forensic science and deepfake detection; (iii) electronic evidence and evidentiary law; and (iv) comparative AI governance. Collectively, these strands provide valuable insights into the technological and legal challenges posed by generative AI while simultaneously revealing substantial gaps concerning judicial treatment of AI-generated evidence in India.

The first body of literature focuses on the transformation of identity theft through advances in artificial intelligence. Traditional identity theft generally involved the unlawful acquisition and misuse of personal information through phishing attacks, database breaches, or document forgery. Contemporary research demonstrates that generative AI has fundamentally altered this paradigm by enabling the creation of synthetic identities that closely replicate the facial features, voice, behavioural patterns, and biometric characteristics of real individuals. Chesney and Citron argue that deepfake technologies have significantly lowered the barriers to sophisticated impersonation, enabling malicious actors to produce highly convincing fabricated content with

minimal technical expertise. Similarly, Farid observes that AI-generated synthetic media increasingly challenge society's ability to distinguish authentic digital information from fabricated content, thereby undermining trust in digital communications and judicial processes.

Recent studies further indicate that AI-assisted identity fraud extends beyond individual victimisation to encompass financial fraud, political misinformation, cyber extortion, online harassment, and organised cybercrime. Maras and Alexandrou emphasise that the growing availability of open-source AI tools has democratised sophisticated cyber deception techniques previously available only to highly skilled actors. Researchers therefore contend that AI-generated identity theft represents not merely a technological advancement but a qualitative transformation in the nature of cybercrime itself.

A second stream of literature concentrates upon digital forensic science and the detection of AI-generated synthetic media. Computer scientists have developed numerous forensic methodologies designed to identify manipulated digital content through image analysis, metadata examination, frequency-domain analysis, facial landmark inconsistencies, biological signal detection, and machine learning-based classification models. Studies by Verdoliva, Farid, and Goyal *et al*. demonstrate considerable progress in detecting deepfake videos by analysing subtle physiological inconsistencies such as unnatural blinking patterns, irregular eye reflections, inconsistent lighting, and spectral artefacts generated during synthetic image creation.

Despite these technological advances, forensic scholars consistently recognise an ongoing technological "arms race" between AI generation and AI detection systems. Every improvement in forensic detection algorithms is rapidly countered by increasingly sophisticated generative models capable of circumventing existing detection mechanisms. Consequently, no presently available forensic tool guarantees absolute certainty regarding the authenticity of AI-generated content. This limitation has profound implications for evidentiary law because judicial proceedings traditionally require expert evidence possessing demonstrable scientific reliability and recognised standards of accuracy.

The third body of scholarship examines the admissibility and authentication of electronic evidence within the Indian legal system. Prior to the enactment of the Bharatiya Sakshya Adhiniyam, 2023[3] (BSA), legal scholarship predominantly centred upon Section 65B of the Indian Evidence Act, 1872, which governed the admissibility of electronic records. Judicial interpretation of this provision evolved considerably through landmark Supreme Court decisions including *Anvar P.V. v. P.K. Basheer*, *Shafhi Mohammad v. State of Himachal Pradesh*, and ultimately *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. These judgments collectively established that electronic evidence ordinarily requires a statutory certificate verifying its authenticity before being admitted into evidence.

Although the Bharatiya Sakshya Adhiniyam, 2023[3] modernises several aspects of evidentiary law and explicitly recognises electronic and digital records, academic commentators argue that it substantially preserves the certificate-based authentication model inherited from Section 65B. Datt and Sharma contend that while the BSA reflects procedural modernisation, it does not fundamentally reconsider the evidentiary assumptions underlying digital authentication in the era of artificial intelligence. Existing scholarship therefore suggests that contemporary evidentiary rules remain better suited to conventional electronic records than to AI-generated synthetic media capable of sophisticated manipulation.

Another significant theme within the literature concerns comparative regulation of artificial intelligence across different jurisdictions. The enactment of the European Union Artificial Intelligence Act, 2024[34] represents one of the most comprehensive attempts to regulate AI systems through a risk-based framework. The legislation imposes transparency obligations requiring providers of AI-generated content to disclose synthetic media and establishes enhanced compliance obligations for high-risk AI applications. Legal scholars regard the EU approach as particularly significant because it shifts regulatory responsibility toward AI developers and deployers rather than relying exclusively upon post hoc judicial determination.

By contrast, the United States has adopted a fragmented regulatory model characterised by sector-specific legislation and state-level initiatives addressing deepfakes, election integrity, consumer protection, and non-consensual intimate imagery. Although federal agencies such as the Federal Trade Commission have increasingly relied upon consumer protection laws to regulate deceptive AI practices, scholars observe that the absence of a comprehensive federal AI statute has produced considerable inconsistency in legal standards across jurisdictions. Comparative literature consequently demonstrates that governments worldwide continue to experiment with different regulatory approaches while confronting similar technological challenges.

Indian scholarship concerning AI regulation has thus far concentrated primarily upon privacy, data protection, intermediary liability, and ethical governance under the Digital Personal Data Protection Act, 2023[5]. Comparatively little attention has been devoted to the evidentiary implications of AI-generated content within criminal proceedings. Existing legal analyses generally examine cybercrime from the perspective of substantive criminal offences without critically evaluating the procedural challenges associated with authenticating AI-generated digital evidence before courts. Furthermore, very few studies integrate forensic science, evidentiary doctrine, constitutional principles, and comparative AI regulation into a unified analytical framework.

A further limitation within the current literature is the relative absence of empirical research concerning institutional preparedness within the Indian criminal justice system. There remains limited scholarly examination of the technological capacity of forensic science laboratories, investigative agencies, prosecutors, and judicial officers to identify, authenticate, and evaluate AI-generated evidence. Questions concerning judicial competence, forensic infrastructure, cross-border cooperation, algorithmic transparency, and expert witness standards remain largely unexplored despite their increasing practical significance.

Accordingly, this study seeks to address four principal gaps in the existing literature. First, it provides a comprehensive doctrinal analysis of the Bharatiya Sakshya Adhiniyam, 2023[3] in the context of AI-generated digital evidence. Secondly, it integrates developments in computer science and digital forensic research with evidentiary principles governing admissibility before Indian courts. Thirdly, it

critically evaluates Indian law through comparative analysis of international AI regulatory frameworks, particularly the European Union Artificial Intelligence Act, 2024[34] and selected United States legislative initiatives. Finally, the study proposes practical legal and institutional reforms designed to strengthen India's capacity to respond effectively to AI-generated identity theft while preserving fairness, reliability, and public confidence in the administration of justice.

By bridging technological scholarship, evidentiary law, comparative regulation, and judicial practice, this research contributes to an emerging field of interdisciplinary legal scholarship that is likely to become increasingly significant as generative artificial intelligence continues to transform both cybercrime and the administration of justice.

Research Methodology

This study adopts a doctrinal legal research methodology supported by comparative legal analysis to examine the emerging challenges posed by AI-generated identity theft and digital evidence within the Indian criminal justice system. Doctrinal research is particularly appropriate because the subject primarily concerns statutory interpretation, judicial precedents, evidentiary principles, and regulatory frameworks governing artificial intelligence, cybercrime, and electronic evidence. Unlike empirical studies that rely upon surveys or interviews, doctrinal research seeks to identify, analyse, interpret, and critically evaluate the existing legal framework in order to assess its adequacy in responding to new technological developments.

The study is based exclusively on qualitative research methods, involving an extensive examination of primary and secondary legal materials. Primary sources include the Constitution of India, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023[2, 6] (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023[1] (BNSS), the Bharatiya Sakshya Adhiniyam, 2023[1] (BSA), the Digital Personal Data Protection Act, 2023[5], judicial decisions of the Supreme Court of India and various High Courts, parliamentary debates, government notifications, and regulatory advisories issued by the Ministry of Electronics and Information Technology (MeitY). These sources collectively establish the current legal position concerning identity theft, electronic evidence, digital investigations, and AI-related offences.

Secondary sources comprise peer-reviewed journal articles, scholarly books, reports published by international organisations such as INTERPOL, Europol, the Organisation for Economic Co-operation and Development (OECD), UNESCO, the Global Partnership on Artificial Intelligence (GPAI), and research publications relating to digital forensics, cybersecurity, and AI governance. Comparative legal materials, including the European Union Artificial Intelligence Act, 2024[34] and selected legislative developments within the United States, have also been examined to identify international best practices capable of informing future reforms within the Indian legal system.

The research employs comparative legal analysis as an important methodological tool. Comparative examination enables evaluation of India's existing regulatory framework against jurisdictions that have already introduced AI-specific legal standards. Particular attention is devoted to transparency obligations, authentication standards, forensic verification mechanisms, judicial oversight, and regulatory accountability established under the European Union AI Act. Selected developments within the United States have similarly been analysed to illustrate alternative approaches towards regulating synthetic media, biometric impersonation, consumer protection, and election-related deepfakes. Comparative analysis facilitates identification of legislative innovations that may appropriately be adapted within the Indian legal context while recognising constitutional, institutional, and technological differences among jurisdictions.

The study further incorporates case-law analysis to examine the evolution of judicial reasoning concerning electronic evidence and AI-generated content. Landmark Supreme Court decisions including Anvar P.V. v. P.K. Basheer, Shafhi Mohammad v. State of Himachal Pradesh, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal have been critically analysed to understand the development of evidentiary principles governing electronic records. More recent High Court decisions involving personality rights, deepfake technologies, and AI-generated synthetic media have also been examined to identify emerging judicial trends concerning artificial intelligence and digital evidence.

Analytical interpretation constitutes another important methodological component. Rather than merely describing statutory provisions, the study critically evaluates their practical effectiveness in addressing AI-generated identity theft. Particular emphasis is placed upon identifying legislative gaps, institutional limitations, forensic challenges, and procedural ambiguities that affect judicial determination of AI-generated evidence. This critical approach enables the formulation of practical recommendations for legislative reform, judicial capacity-building, forensic infrastructure, and international cooperation.

Notwithstanding its comprehensive doctrinal scope, the present study acknowledges certain limitations. First, AI-related litigation in India remains relatively limited because generative artificial intelligence has emerged only recently as a widespread technological phenomenon. Consequently, judicial precedents specifically addressing AI-generated identity theft remain scarce. Secondly, the study does not incorporate empirical interviews with judges, prosecutors, forensic scientists, law enforcement officers, or cybersecurity professionals. Such empirical investigation would provide valuable practical insights into institutional challenges associated with AI-generated evidence. Thirdly, technological developments within artificial intelligence continue to evolve rapidly, meaning that legislative and judicial responses discussed herein may require periodic reassessment as newer forms of synthetic media emerge.

Despite these limitations, the adopted doctrinal and comparative methodology provides a robust analytical framework for evaluating the adequacy of existing Indian law while simultaneously identifying reforms necessary to strengthen judicial responses to AI-generated identity theft and digital evidence.

Results and Discussion

This section analyses the legal, evidentiary, and institutional challenges posed by AI-generated identity theft in India. It evaluates the adequacy of existing laws, authentication standards under the Bharatiya Sakshya Adhiniyam, 2023[3], forensic capabilities, judicial responses, and comparative international approaches to identify key gaps and recommend effective legal reforms.

1. Inadequacy of the Existing Legal Framework for AI-Generated Identity Theft

The analysis reveals that India's existing legal framework is insufficient to address the emerging challenges of AI-generated identity theft and synthetic digital identities. Sections 66C and 66D of the Information Technology Act, 2000[6] criminalise identity theft and cheating by personation; however, these provisions were enacted before the rise of generative artificial intelligence and primarily target conventional cybercrimes involving passwords, electronic signatures, and unique identification credentials. Modern AI systems can generate synthetic identities, cloned voices, deepfake videos, and fabricated biometric profiles that often do not involve the direct theft of an existing person's identity, thereby creating significant legal uncertainty. Similarly, although the Bharatiya Nyaya Sanhita, 2023[2] contains provisions relating to forgery, cheating, and impersonation, these offences continue to reflect traditional concepts of fraud rather than AI-enabled identity manipulation. The absence of statutory definitions relating to deepfakes, synthetic identities, biometric spoofing, and algorithmic impersonation limits effective investigation and prosecution. Consequently, India's present legal framework requires targeted legislative reform capable of addressing the scale, automation, and technological sophistication associated with AI-generated identity crimes.

2. Authentication Challenges under the Bharatiya Sakshya Adhiniyam, 2023[3]

The Bharatiya Sakshya Adhiniyam, 2023[3] modernises India's evidentiary law by recognising electronic records as admissible evidence. Nevertheless, the study demonstrates that its certificate-based authentication framework remains inadequate when applied to AI-generated digital evidence. Sections 61, 63, and 65 largely preserve the evidentiary principles previously contained in Section 65B of the Indian Evidence Act, requiring certification regarding the production and integrity of electronic records. While effective for conventional digital documents, these provisions cannot independently establish whether AI-generated videos, images, or voice recordings genuinely represent real events or merely constitute synthetic fabrications. AI-generated content frequently lacks a clearly identifiable creator or custodian, making conventional certification difficult. Moreover, forensic verification increasingly depends upon metadata analysis, blockchain preservation, and AI-detection technologies rather than documentary certification alone. The distinction between technical integrity and factual authenticity therefore becomes critical. Existing evidentiary rules require significant reform to incorporate AI-specific authentication standards capable of ensuring fairness, reliability, and judicial confidence in digital evidence.

3. Digital Forensics and AI Detection: Institutional Challenges

Digital forensic science plays a crucial role in determining the authenticity of electronic evidence. However, the findings indicate that India's forensic infrastructure remains inadequately prepared to investigate AI-generated identity crimes. Traditional forensic laboratories primarily examine mobile devices, computers, deleted files, and financial cybercrime, whereas AI-generated evidence requires specialised expertise in deepfake detection, biometric analysis, metadata reconstruction, machine-learning algorithms, and computer vision technologies. State Forensic Science Laboratories continue to face shortages of trained personnel, outdated equipment, and limited AI-specific capability. Furthermore, no nationally accepted forensic standards currently exist for examining synthetic media, resulting in inconsistent methodologies across laboratories.

4. Judicial Responses and Comparative Perspectives

Indian courts have begun recognising the legal implications of AI-generated content, although judicial responses remain limited. Decisions such as *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* reaffirm procedural requirements for electronic evidence but do not specifically address generative AI. More recent High Court decisions concerning AI-generated misuse of personality rights, including the Bombay High Court's protection of Asha Bhosle's voice and likeness and the Delhi High Court's intervention against fabricated videos of Shashi Tharoor, indicate growing judicial awareness of synthetic media. Comparative analysis further demonstrates that the European Union AI Act, 2024[29] adopts a proactive regulatory approach through mandatory transparency obligations for AI-generated content, while the United States has pursued sector-specific regulation through state legislation and regulatory enforcement. These international developments provide valuable guidance for India. The study therefore recommends comprehensive AI legislation, AI-specific evidentiary standards under the Bharatiya Sakshya Adhiniyam, strengthened forensic infrastructure, specialised judicial training, and enhanced international cooperation to ensure that Indian courts remain capable of addressing the rapidly evolving challenges posed by AI-generated identity theft and digital evidence.

Recommendations

The findings of this study indicate that although India has modernised its criminal justice framework through the Bharatiya Nyaya Sanhita, 2023[2] (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023[1] (BNSS), and Bharatiya Sakshya Adhiniyam, 2023[1] (BSA), these statutes do not adequately address the emerging challenges posed by AI-generated identity theft and synthetic digital evidence. To strengthen the legal and institutional response, five key recommendations are proposed.

First, India should enact a comprehensive Artificial Intelligence Regulation Act that specifically criminalises AI-enabled identity theft, deepfakes, voice cloning, biometric impersonation, and synthetic media misuse. The legislation should impose liability on creators and distributors of malicious AI-generated content and require transparency measures such as digital watermarking and traceability.

Second, the Bharatiya Sakshya Adhiniyam, 2023[3] should be amended to introduce AI-specific evidentiary standards. Courts should adopt a multi-layered authentication framework incorporating metadata verification, blockchain-based evidence preservation, forensic examination by accredited laboratories, and independent expert certification to establish the authenticity of AI-generated electronic evidence.

Third, India should substantially strengthen its digital forensic infrastructure by establishing specialised AI

forensic laboratories equipped with advanced deepfake detection technologies, AI-assisted investigation tools, secure digital evidence repositories, and nationally standardised forensic protocols. Continuous technological upgrades and collaboration with leading research institutions should also be encouraged.

Fourth, specialised capacity-building programmes should be introduced for judges, prosecutors, investigating officers, and forensic experts. Judicial academies and law enforcement agencies should provide regular training on artificial intelligence, digital forensics, deepfake detection, blockchain technology, and scientific evaluation of expert evidence to ensure effective adjudication of AI-related cases.

Finally, India should enhance international cooperation through organisations such as INTERPOL, GPAI, UNESCO, OECD, and UNODC to facilitate cross-border investigations, information sharing, harmonisation of AI governance standards, and collaborative research. A coordinated legal, technological, and institutional approach is essential to preserve the integrity of digital evidence, protect individual rights, and strengthen public confidence in the administration of justice in the age of artificial intelligence.

Conclusion

Artificial intelligence has transformed the nature of identity theft and digital evidence, creating significant challenges for the Indian criminal justice system. The rapid development of deepfakes, synthetic media, voice cloning, and AI-generated identities has undermined the traditional reliability of electronic evidence, making authentication and forensic verification increasingly complex. This study demonstrates that although the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023[2, 6], the Bharatiya Nagarik Suraksha Sanhita, 2023[1], and the Bharatiya Sakshya Adhiniyam, 2023[1] provide a legal framework for addressing cybercrime and electronic evidence, they are not fully equipped to deal with the unique evidentiary challenges posed by generative AI. The continued reliance on certificate-based authentication under the BSA, 2023 is insufficient to verify the authenticity of AI-generated content, highlighting the need for AI-specific evidentiary standards and advanced forensic verification mechanisms.

The study further identifies deficiencies in forensic infrastructure, judicial expertise, and institutional preparedness, which limit the effective investigation and adjudication of AI-enabled identity crimes. Drawing upon comparative developments, particularly the European Union AI Act, the paper recommends legislative reforms, strengthened forensic capabilities, specialised judicial training, and international cooperation. A balanced regulatory framework that promotes technological innovation while ensuring evidentiary integrity, procedural fairness, and constitutional safeguards is essential to protect the administration of justice in the evolving era of artificial intelligence.

References

1. Bharatiya Nagarik Suraksha Sanhita (Act No. 46 of 2023), 2023.
2. Bharatiya Nyaya Sanhita (Act No. 45 of 2023), 2023.
3. Bharatiya Sakshya Adhiniyam (Act No. 47 of 2023), 2023.
4. Constitution of India, 1950.
5. Digital Personal Data Protection Act (Act No. 22 of 2023), 2023.
6. Information Technology Act (Act No. 21 of 2000), 2000.
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), 2024.
8. Anvar P.V. v. P.K. Basheer. SCC,2014:10:473.
9. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. SCC,2020:7:1.
10. Shafhi Mohammad v. State of Himachal Pradesh. SCC,2018:2:801.
11. State (NCT of Delhi) v. Navjot Sandhu. SCC,2005:11:600.
12. Asha Bhosle v. Google LLC & Others. Bombay High Court, Interim Order, 2024.
13. Shashi Tharoor v. X Corp & Others. Delhi High Court, 2024.
14. Casey E. Digital Evidence and Computer Crime (4th ed.). Academic Press, 2020.
15. Goodfellow I, Bengio Y, Courville A. Deep Learning. MIT Press, 2016.
16. Hutchinson T. Researching and Writing in Law (5th ed.). Thomson Reuters, 2022.
17. Russell S, Norvig P. Artificial Intelligence: A Modern Approach (4th ed.). Pearson, 2021.
18. Wall DS. Cybercrime: The Transformation of Crime in the Information Age (3rd ed.). Polity Press, 2021.
19. Chesney R, Citron DK. Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review,2019:107(6):1753–1820.
20. Citron DK. Sexual privacy. Yale Law Journal,2020:128(7):1870–1960.
21. Datt A, Sharma R. Electronic evidence in India: From Section 65B to the Bharatiya Sakshya Adhiniyam. NUJS Law Review,2024:16(1):1–35.
22. Farid H. Creating, using, misusing, and detecting deepfakes. Journal of Online Trust and Safety,2022:8(1):1–18.
23. Goyal R, Singh A, Kumar S. Deepfake detection: A systematic literature review. Expert Systems with Applications,2023:218:119616.
24. Maras MH, Alexandrou A. Determining authenticity of video evidence in the age of deepfakes. Harvard Journal of Law & Technology,2019:32(2):275–310.
25. Verdoliva L. Media forensics and deepfake detection: An overview. IEEE Journal of Selected Topics in Signal Processing,2020:14(5):910–932.
26. Westerlund M. The emergence of deepfake technology: A review. Technology Innovation Management Review,2019:9(11):40–53.
27. Whittaker M, et al. AI Now Report 2018. AI Now Institute, New York University, 2018.
28. Ministry of Electronics and Information Technology. Advisory to Intermediaries on Deepfakes. Government of India, 2023.
29. Ministry of Electronics and Information Technology. Advisory on Responsible AI and Synthetic Media. Government of India, 2024.
30. Press Information Bureau. Government Measures to Combat Deepfakes. Government of India, 2024.
31. Law Commission of India. Report on Criminal Law Reforms. Government of India, 2023.

32. Europol. Facing Reality? Law Enforcement and the Challenge of Deepfakes. Europol Publications Office, 2022.
33. Global Partnership on Artificial Intelligence (GPAI). Synthetic Media: Detection, Regulation and Societal Impact, 2023.
34. INTERPOL. Artificial Intelligence Toolkit for Law Enforcement, 2024.
35. OECD. Artificial Intelligence, Digital Economy and Society. OECD Publishing, 2024.
36. UNESCO. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021.
37. United Nations Office on Drugs and Crime. Cybercrime and Artificial Intelligence. UNODC, 2023.
38. World Economic Forum. Global Risks Report 2024. WEF, 2024.
39. National Crime Records Bureau. Crime in India 2023. https://ncrb.gov.in, 2024.
40. National Cyber Crime Reporting Portal. https://cybercrime.gov.in,2024.
41. Reserve Bank of India. Annual Report 2023–24. https://rbi.org.in,2024.
42. Supreme Court of India. https://www.sci.gov.in,2024.