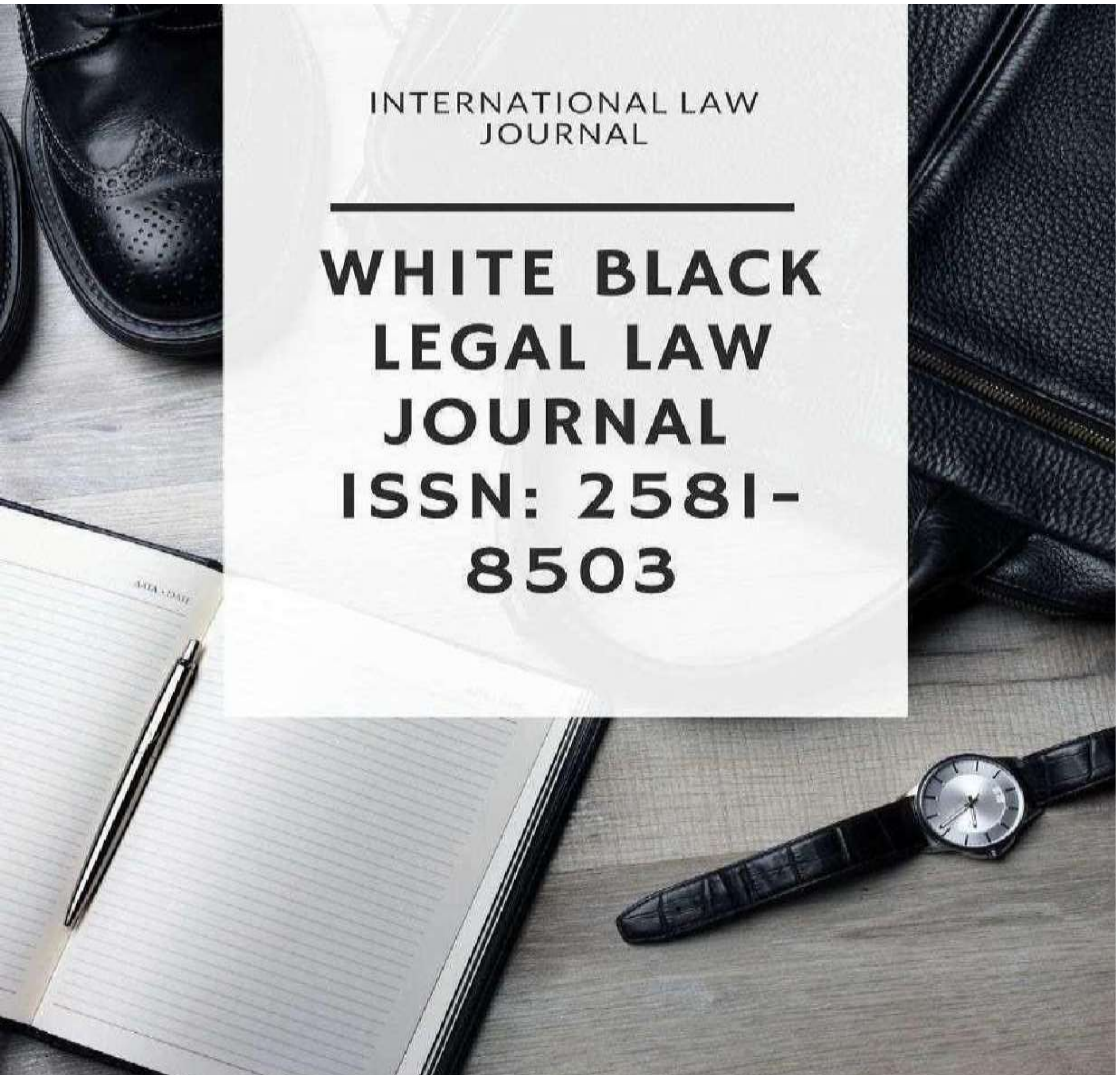

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DEEPFAKE EVIDENCE AND THE CRISIS OF AUTHENTICITY IN INDIAN COURTROOMS

AUTHORED BY - DR. GARIMA YADAV
Assistant Professor
Anangpuria Law School, Faridabad

CO-AUTHOR - MR. HARBIR SINGH
Research Scholar (LL.M.)
Anangpuria Law School, Faridabad
Affiliated to Maharshi Dayanand University, Rohtak

Abstract

The increasing reliance of Indian courts on electronic evidence has coincided with rapid advancements in artificial intelligence, particularly the emergence of deepfake technology. Deepfakes—AI-generated synthetic audio and visual content—pose a serious challenge to the foundational evidentiary principles of authenticity and reliability. This paper critically examines the implications of deepfake evidence within Indian courtrooms, with specific reference to Section 65B of the Indian Evidence Act, 1872(Now Section 63 of Bharatiya Sakshya Adhiniyam 2023). Through doctrinal legal analysis and comparative evaluation of global regulatory responses, the study demonstrates that procedural compliance under existing law is insufficient to address the risks posed by sophisticated synthetic media. It argues that deepfakes threaten not only evidentiary integrity but also constitutional values such as fair trial, privacy, and public confidence in the judiciary. The paper proposes targeted legislative reforms, standardised admissibility protocols, enhanced forensic infrastructure, and judicial capacity-building as necessary safeguards for preserving justice in the digital era.

Keywords: Deepfake Evidence, Electronic Records, Section 65B, Indian Evidence Act, Section 63 Bharatiya Sakshya Adhiniyam, Artificial Intelligence, Criminal Justice

1. Introduction

The administration of justice depends fundamentally upon the credibility of evidence placed before courts. Traditionally, visual and audio records have been regarded as highly persuasive forms of proof, operating on the assumption that such records represent objective reality. In India, this assumption has gained further significance with the increasing judicial reliance on electronic evidence such as CCTV footage, mobile phone recordings, and digital documents. To regulate this shift, Section 65B of the Indian Evidence Act, 1872(Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) was introduced, prescribing procedural safeguards for the admissibility of electronic records.

However, recent developments in artificial intelligence have destabilised this evidentiary confidence. Deepfake technology enables the creation of synthetic audio-visual content that can convincingly replicate real individuals, rendering traditional indicators of authenticity unreliable. Unlike conventional forms of digital manipulation, deepfakes are generated through complex machine learning models capable of producing near-indistinguishable fabrications. In such a context, the long-standing judicial maxim that "seeing is believing" no longer holds true. The implications of this technological shift are particularly acute for the Indian legal system. Courts continue to emphasise procedural compliance under Section 65B(Now Section 63 of Bharatiya Sakshya Adhiniyam 2023), as reflected in landmark Supreme Court decisions, yet these safeguards are ill-equipped to detect substantively fabricated but procedurally valid evidence. The risk of wrongful convictions, erosion of fair trial guarantees, and declining public trust necessitates a critical re-evaluation of existing evidentiary frameworks.

This paper seeks to analyse the challenges posed by deepfake evidence in Indian courtrooms by examining its technical foundations, judicial treatment of electronic evidence, ethical and societal implications, and comparative global responses. It argues that Indian evidentiary law must evolve beyond formal certification requirements and incorporate substantive authenticity checks to ensure that technological progress does not undermine the pursuit of justice.

2. Technical Foundations of Deepfakes

Deepfake technology represents a qualitative shift from traditional forms of digital manipulation. Earlier techniques such as manual video editing or audio splicing often left visible or audible traces that could be identified through conventional forensic examination.

Deepfakes, by contrast, are generated through advanced artificial intelligence models that learn and replicate complex human features, including facial expressions, body movements, and vocal patterns. This technological sophistication makes deepfakes particularly problematic in judicial contexts where evidentiary reliability is paramount.

At the core of deepfake creation are deep learning architectures trained on extensive datasets. Generative Adversarial Networks (GANs) are among the most widely used models. GANs function through a dual-network system comprising a generator, which creates synthetic content, and a discriminator, which evaluates its authenticity. Through repeated iterations, the generator progressively improves until the synthetic output becomes nearly indistinguishable from genuine media. This adversarial process enables the production of hyper-realistic videos and images capable of deceiving both human observers and conventional forensic tools.

Another commonly employed technique involves auto-encoders, which compress and reconstruct data to map one individual’s facial features onto another’s body. Voice synthesis and cloning technologies similarly rely on deep neural networks trained to analyse pitch, tone, cadence, and linguistic patterns. These tools can generate audio recordings that convincingly imitate real individuals, posing serious risks in cases involving confessions, threats, or telephonic communications.

From a legal perspective, the danger posed by deepfakes lies not merely in their existence but in their accessibility. Open-source software, consumer applications, and online platforms have significantly lowered the barrier to creating synthetic media. In the Indian context—where digital evidence is frequently relied upon and forensic resources are unevenly distributed—this accessibility magnifies the risk of misuse within criminal and civil proceedings.

Equally concerning are the limitations of existing detection mechanisms. While researchers have developed AI-based detection tools that analyse pixel inconsistencies, facial micro-expressions, or audio artefacts, these tools remain imperfect and are engaged in a continuous technological race with deepfake creators. As detection improves, generation techniques adapt, rendering static forensic standards ineffective. This dynamic underscores the necessity for courts to adopt a cautious and informed approach when evaluating audiovisual evidence in the age of artificial intelligence.

3. Evidentiary Standards and Judicial Challenges in India

3.1 Statutory Framework Governing Electronic Evidence

The Indian Evidence Act, 1872(Now Bharatiya Sakshya Adhiniyam, 2023) provides the foundational framework for determining the admissibility of evidence in judicial proceedings. With the increasing use of digital records, Section 65B (Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) was introduced to regulate electronic evidence by prescribing procedural conditions intended to ensure authenticity and integrity. These conditions include certification regarding the manner of production of the electronic record, the functioning of the device used, and assurances against tampering.

Judicial interpretation of Section 65B (Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) has consistently emphasised strict compliance. In Anvar P.V. v. P.K. Basheer (2014), the Supreme Court categorically held that electronic evidence is inadmissible in the absence of the statutory certificate. This position was reaffirmed and clarified in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), wherein the Court rejected any dilution of the mandatory certification requirement. More recently, in Chandrabhan Sudam Sanap v. State of Maharashtra (2025), the Supreme Court reiterated that a certificate under Section 65B(4) (Now Section 63(4) of Bharatiya Sakshya Adhiniyam 2023) constitutes a condition precedent for admissibility, even in serious criminal cases involving CCTV footage.

These decisions reflect a strong judicial commitment to procedural safeguards. However, they also reveal a critical limitation: Section 65B (Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) addresses the manner of production of electronic records but does not engage with the substantive question of whether the content itself is genuine or synthetically fabricated.

3.2 Deepfakes and the Crisis of Authenticity

Deepfake evidence exposes a structural vulnerability within the existing evidentiary regime. A synthetically generated video or audio recording may satisfy all procedural requirements under Section 65B (Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) while remaining entirely fabricated. In such cases, certification functions as a formal compliance mechanism rather than a substantive guarantee of truth.

This creates significant challenges for judges tasked with determining admissibility and evidentiary weight. Most judges are not trained in advanced artificial intelligence or digital forensics, and courts often lack access to specialised forensic expertise. The absence of clear judicial guidelines further exacerbates uncertainty, resulting in inconsistent approaches across jurisdictions.

3.3 Equality, Fair Trial, and Institutional Credibility

The implications of deepfake evidence extend beyond technical admissibility. Resource disparities between litigants may allow well-funded parties to exploit advanced technologies or forensic experts, thereby undermining the principle of equality before law. From a constitutional perspective, the risk of wrongful convictions or acquittals implicates the right to a fair trial under Articles 14 and 21 of the Constitution.

Moreover, continued reliance on procedurally certified yet substantively unreliable evidence threatens public confidence in the judicial process. If courts are perceived as incapable of distinguishing truth from technological fabrication, the legitimacy of judicial outcomes may be called into question. These concerns underscore the urgent need to reorient evidentiary standards towards substantive authenticity rather than formal compliance alone.

4. Ethical and Societal Implications

The challenge posed by deepfake evidence is not confined to procedural or technical concerns; it raises profound ethical and societal questions that strike at the core of the justice system. Courts are moral institutions entrusted with protecting dignity, liberty, and public confidence. The introduction of synthetic media into judicial proceedings risks undermining these foundational values.

4.1 Privacy and Human Dignity

Privacy has been recognised as a fundamental right under Article 21 of the Constitution, most notably in Justice K.S. Puttaswamy v. Union of India (2017). Deepfakes threaten this right by enabling the creation of fabricated videos or audio recordings that depict individuals in compromising or criminal contexts. Even where such material is ultimately discredited, the harm to reputation, dignity, and psychological well-being is often irreversible.

In courtroom settings, the admission of deepfake evidence may compel individuals to relive fabricated narratives under the authority of law. This raises serious ethical concerns regarding consent, dignity, and the proportionality of evidentiary intrusion, particularly in cases involving personal relationships, political speech, or alleged confessions.

4.2 Risk of Wrongful Convictions

The persuasive power of audio-visual evidence is well documented. Deepfakes exploit this cognitive bias by presenting fabricated events as seemingly objective reality. In criminal trials, especially those relying on CCTV footage or recorded communications, manipulated evidence may result in wrongful convictions or unjust acquittals.

From an ethical standpoint, the possibility that an individual may be deprived of liberty on the basis of synthetic evidence represents a grave miscarriage of justice. The moral responsibility borne by judges and prosecutors to prevent such outcomes necessitates heightened scrutiny and scepticism when evaluating digital media.

4.3 Media Influence and Trial by Public Opinion

The societal impact of deepfakes is amplified by rapid dissemination through social media platforms. Viral synthetic content often shapes public narratives long before judicial proceedings conclude, giving rise to the phenomenon of ‘trial by media’. Such external pressures risk compromising judicial impartiality and infringing upon the presumption of innocence.

In India, where digital platforms play a central role in public discourse, deepfakes can inflame social tensions, influence witnesses, and undermine the integrity of the adjudicatory process. Ethical adjudication therefore requires courts to actively resist the influence of unverified digital narratives.

4.4 Public Trust in Judicial Institutions

Public confidence in the judiciary depends on the belief that legal outcomes are grounded in truth and fairness. If courts are perceived as unable to distinguish authentic evidence from technological fabrication, institutional legitimacy may be eroded. The ethical obligation to preserve public trust thus extends beyond individual cases and demands systemic safeguards against synthetic deception.

5. Legal Responses in India and Comparative Perspectives

5.1 Indian Legal and Regulatory Responses

India’s response to the challenge of deepfakes remains fragmented. While the Information Technology Act, 2000 addresses certain forms of digital misuse, it does not explicitly regulate synthetic media. The Information Technology (Intermediary Guidelines and Digital Media

Ethics Code) Rules, 2021 impose content moderation obligations on intermediaries, yet their focus is primarily on misinformation, obscenity, and public order rather than evidentiary integrity.

Judicial education initiatives have begun to acknowledge the challenges of electronic evidence, but specialised training on artificial intelligence and deepfake detection remains limited. Consequently, courts continue to rely heavily on procedural certification under Section 65B, without corresponding substantive verification mechanisms.

5.2 Comparative Approaches

A comparative perspective offers valuable insights. In the United States, courts increasingly rely on expert testimony and forensic authentication to assess the reliability of digital evidence. Several states have enacted targeted legislation addressing malicious deepfake use, particularly in electoral and non-consensual content contexts.

The European Union adopts a regulatory approach grounded in transparency and data protection. The proposed Artificial Intelligence Act mandates disclosure obligations for synthetic media, while the General Data Protection Regulation provides remedies for privacy violations. China, by contrast, has adopted a stringent model requiring mandatory labelling of synthetic content and imposing strict platform liability.

These divergent approaches illustrate that while no single model offers a complete solution, a combination of expert-driven adjudication, transparency requirements, and regulatory accountability may offer a balanced path forward for India.

6. Recommendations and Future Directions

The challenges identified in this study necessitate a forward-looking and integrated response. Procedural compliance alone cannot safeguard the integrity of judicial outcomes in the age of artificial intelligence.

6.1 Legislative Reform

The Indian Evidence Act should be amended to explicitly address synthetic media. Section 65B (Now Section 63 of Bharatiya Sakshya Adhiniyam 2023) must be supplemented with provisions mandating forensic verification of audio-visual evidence where authenticity is disputed. Similarly, amendments to the Information Technology Act should criminalise malicious deepfake creation while ensuring that restrictions remain proportionate under Article

19(2).

6.2 Standardised Admissibility Protocols

Judicial guidelines should be developed to assist courts in assessing deepfake evidence. These protocols should integrate procedural certification with substantive forensic analysis and expert testimony, thereby promoting consistency and fairness across jurisdictions.

6.3 Forensic Infrastructure and Judicial Training

Investment in forensic infrastructure is essential. Establishing a National Forensic AI Centre and upgrading existing forensic laboratories with advanced detection tools would significantly enhance institutional capacity. Parallely, judicial training programmes must incorporate digital literacy, artificial intelligence, and ethical evaluation of electronic evidence.

6.4 Public Awareness and International Cooperation

Public awareness initiatives aimed at enhancing digital literacy can mitigate the societal impact of deepfakes. Given the cross-border nature of synthetic media, India should also engage in international cooperation to harmonise standards and share technological expertise.

7. Conclusion

Deepfake technology represents a fundamental challenge to traditional evidentiary assumptions within the Indian legal system. While existing statutory frameworks emphasise procedural safeguards for electronic evidence, they are ill-equipped to address the substantive authenticity concerns posed by synthetic media. The risks of wrongful convictions, privacy violations, and erosion of public trust underscore the urgency of reform.

This paper has argued that safeguarding justice in the digital age requires a holistic approach that combines legislative reform, forensic innovation, judicial education, and ethical governance. By evolving its evidentiary standards to meet contemporary technological realities, India can ensure that the pursuit of truth remains central to judicial decision-making, even as artificial intelligence continues to reshape the nature of evidence.

References

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. Chandrabhan Sudam Sanap v. State of Maharashtra, (2025) SCC OnLine SC ___.
4. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
5. Indian Evidence Act 1872, ss 65A–65B.
6. Information Technology Act 2000.
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
8. European Commission, ‘Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)’ COM (2021) 206 final.
9. General Data Protection Regulation (EU) 2016/679.