



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.

ARTIFICIAL INTELLIGENCE, DEEPFAKES, AND THE LAW OF EVIDENCE: AN ANALYSIS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

AUTHORED BY - DR. ARPITA MISHRA

Assistant Professor,
Amity Law School, Amity University, Patna

CO-AUTHOR - DR. KARUNESH SHUKLA

Assistant Professor
Amity Law School, Amity University, Patna

Abstract

The rapid advancement of Artificial Intelligence (AI) has fundamentally transformed the manner in which information is generated, processed, and disseminated across digital platforms. Among the most disruptive innovations is deepfake technology, which employs sophisticated machine learning algorithms to create highly realistic yet fabricated audio, video, and image content. While AI has significantly contributed to advancements in healthcare, education, governance, finance, and law enforcement, its misuse has generated unprecedented challenges for legal systems worldwide, particularly in the realm of evidentiary law. Courts increasingly rely upon electronic evidence for adjudication of civil, criminal, commercial, and constitutional disputes. However, the emergence of AI-generated evidence raises serious concerns regarding authenticity, admissibility, reliability, and the potential manipulation of judicial proceedings.

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) marks a significant reform in India's law of evidence by replacing the century-old Indian Evidence Act, 1872. The legislation expressly recognizes electronic and digital records as documentary evidence and seeks to modernize evidentiary standards in response to technological developments. Nevertheless, despite acknowledging electronic evidence, the Act remains largely silent on AI-generated content, synthetic media, deepfake videos, algorithmic manipulation, and the forensic verification of machine-generated evidence. Consequently, judges, investigators, prosecutors, and forensic experts continue to face considerable uncertainty while determining

the evidentiary value of AI-generated material.

This research critically examines the legal implications of Artificial Intelligence and deepfake technology within the framework of the Bharatiya Sakshya Adhiniyam, 2023. It analyses the statutory provisions governing electronic evidence, evaluates their adequacy in addressing emerging technological threats, and explores constitutional concerns relating to privacy, fair trial, due process, and self-incrimination. The article further examines landmark judicial pronouncements of the Supreme Court of India concerning electronic evidence and compares India's evidentiary framework with contemporary legal developments in the United States, the United Kingdom, the European Union, and Singapore.

The study argues that while the Bharatiya Sakshya Adhiniyam, 2023 represents an important step towards digital modernization, it remains insufficient to regulate AI-generated evidence effectively. The absence of statutory standards for authentication, forensic certification, algorithmic transparency, and deepfake detection creates significant risks for the administration of justice. The paper recommends comprehensive legislative reforms incorporating AI-specific evidentiary standards, mandatory digital forensic protocols, expert certification mechanisms, judicial training, and the adoption of internationally accepted technological safeguards to preserve the integrity of judicial proceedings in the digital age.

Keywords: Artificial Intelligence, Deepfakes, Electronic Evidence, Bharatiya Sakshya Adhiniyam, Digital Forensics, Admissibility, Authentication, Machine Learning, Criminal Justice, Constitutional Law.

1. Introduction

Technological innovation has consistently shaped the evolution of legal institutions. From handwritten manuscripts to electronic documents, and from oral testimony to digital recordings, the law of evidence has continually adapted to accommodate new forms of information. The twenty-first century, however, presents a fundamentally different challenge. Artificial Intelligence¹ is no longer merely an assistive technology but has become capable of independently generating text, audio, photographs, videos, voice recordings, contracts, legal

¹ Radha Ranjan, Jivantika Gulati "Catalytic Role of Artificial Intelligence in Ameliorating Criminal Justice System: A Critical Analysis" in *Empowerment and Equality: Navigating Human Rights Law in a Complex World* 47–54 (Institute of Legal Education, Tamil Nadu, 2023).

documents, and even human-like interactions. While these developments have significantly enhanced productivity and innovation, they have simultaneously created serious concerns regarding the authenticity and reliability of evidence presented before courts.²

Artificial Intelligence refers to computational systems capable of performing tasks that ordinarily require human intelligence, including learning, reasoning, decision-making, language processing, pattern recognition, and predictive analysis. Recent advancements in machine learning and deep neural networks have enabled AI systems to produce synthetic media that closely resemble authentic human speech and appearance. One of the most controversial applications of AI is deepfake technology, which utilizes Generative Adversarial Networks (GANs) to manipulate digital content in a manner that is often indistinguishable from reality. Unlike traditional digital editing techniques, deepfakes possess an extraordinary capacity to fabricate highly convincing visual and audio recordings capable of misleading investigators, courts, and the general public.³

The legal implications of deepfake technology extend beyond misinformation and social media manipulation. In criminal investigations, fabricated surveillance footage may falsely implicate innocent individuals.⁴ In civil litigation, manipulated electronic communications may distort contractual obligations or commercial transactions. Within electoral processes, deepfake videos may undermine democratic institutions by disseminating false political narratives. The possibility that fabricated evidence may enter judicial proceedings presents one of the most significant challenges confronting contemporary evidence law.⁵

India's judicial system has witnessed an exponential increase in reliance upon electronic evidence over the past two decades. Mobile phone recordings, CCTV footage, emails, WhatsApp conversations, cloud storage, GPS records, biometric data, blockchain records, and digital signatures now constitute essential forms of documentary evidence. Recognizing these technological developments, Parliament enacted the Bharatiya Sakshya Adhiniyam, 2023, replacing the colonial-era Indian Evidence Act, 1872. The new legislation reflects the

² Ian Goodfellow et al., "Generative Adversarial Networks" (2014) *Advances in Neural Information Processing Systems*.

³ Russell Stuart & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

⁴ Bheem Singh Meena, Radha Ranjan & Shyam Kumar Anand, "Virtual Meetings Under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era", 4(2) *ShodhKosh: Journal of Visual and Performing Arts* 1256–1263 (2023).

⁵ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

legislative intention to modernize evidentiary principles by expressly incorporating electronic and digital records within the definition of documentary evidence and harmonizing the law with technological advancements.

Despite these reforms, the Bharatiya Sakshya Adhiniyam remains largely focused on conventional electronic records rather than AI-generated evidence. The legislation does not define Artificial Intelligence, synthetic media, algorithmic decision-making, or deepfake technology. It also fails to prescribe statutory procedures for verifying the authenticity of AI-generated evidence or determining the reliability of machine-generated outputs. Consequently, judges must continue relying upon traditional principles of admissibility developed under earlier judicial precedents, despite the fundamentally different technological characteristics of AI-generated content.⁶

The challenges posed by AI extend beyond questions of authenticity. Constitutional guarantees under Articles 20 and 21 of the Constitution of India require criminal proceedings to maintain procedural fairness while protecting individual liberty and privacy.⁷ AI-powered surveillance, facial recognition technologies, predictive policing, biometric identification systems, and automated evidence generation raise complex constitutional concerns regarding due process, informational privacy, and protection against self-incrimination.⁸ The Supreme Court has consistently recognized that technological developments cannot override constitutional guarantees merely because they facilitate criminal investigation.⁹ Instead, technological innovation must remain subject to constitutional limitations designed to preserve fairness within the administration of justice.

Internationally, jurisdictions have begun responding to these challenges through legislative and judicial reforms. The European Union has adopted the AI Act, introducing risk-based regulation of artificial intelligence systems. Several American jurisdictions have enacted laws criminalizing malicious deepfake dissemination, particularly in electoral and non-consensual intimate imagery contexts. Singapore has modernized its evidentiary framework to accommodate electronic evidence alongside sophisticated forensic authentication procedures.¹⁰

⁶ Bharatiya Sakshya Adhiniyam, 2023.

⁷ Constitution of India, arts. 20 & 21.

⁸ Information Technology Act, 2000.

⁹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁰ European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689).

The United Kingdom has likewise strengthened digital forensic standards governing electronic evidence in criminal prosecutions. These comparative developments demonstrate an emerging global consensus that traditional evidence law alone cannot adequately regulate AI-generated evidence.¹¹

Against this background, the Bharatiya Sakshya Adhiniyam, 2023 represents both an opportunity and a challenge. While it modernizes India's evidentiary framework by recognizing electronic records, it stops short of comprehensively regulating the rapidly evolving landscape of Artificial Intelligence. This legislative gap may undermine judicial confidence in digital evidence and increase the risk of wrongful convictions, fabricated claims, and procedural injustice.

The present study seeks to critically evaluate whether the Bharatiya Sakshya Adhiniyam, 2023 adequately addresses the evidentiary challenges posed by Artificial Intelligence and deepfake technology. It examines statutory provisions, judicial precedents, constitutional principles, comparative legal developments, and emerging technological practices to determine whether India's evidence law remains capable of preserving fairness, authenticity, and reliability in an increasingly digital justice system.

2. Statement of the Problem

The emergence of Artificial Intelligence (AI) has transformed the creation, storage, and dissemination of information. AI-powered systems can now autonomously generate text, audio, images, videos, and other forms of digital content with remarkable realism. While these technological developments have significantly benefited sectors such as healthcare, finance, governance, education, and law enforcement, they have simultaneously created complex legal challenges concerning the authenticity and reliability of digital evidence. Among the most significant manifestations of AI is deepfake technology, which enables the fabrication of highly realistic audio-visual content capable of misleading individuals, investigators, and judicial authorities. Unlike conventional digital manipulation, deepfakes can imitate human appearance, speech, facial expressions, and mannerisms with extraordinary accuracy, making them increasingly difficult to detect without specialized forensic tools.

¹¹ Gulati, Jivantika & Radha Ranjan, "Cascading Role of Governance in Ensuring Judicial Activism in India", 19(2S) *Bhartiya Journal of Public Administration (BJPA)* (2022).

The legal system traditionally relies upon the principles of authenticity, relevance, admissibility, and reliability while evaluating evidence. These principles assume that documentary and electronic records originate from identifiable human actors and can be verified through conventional methods of authentication. However, AI-generated evidence fundamentally challenges these assumptions because it may be created autonomously, manipulated algorithmically, or altered without leaving visible traces of fabrication. Consequently, judges and investigating agencies face considerable difficulty in determining whether AI-generated content accurately represents reality or has been artificially synthesized to influence judicial outcomes.

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a landmark reform in India's evidentiary framework by replacing the Indian Evidence Act, 1872 and expressly recognizing electronic records as documentary evidence. The legislation seeks to modernize the law in response to technological advancements and the increasing reliance upon digital evidence in judicial proceedings. Nevertheless, despite acknowledging electronic records, the Act does not specifically address the evidentiary implications of Artificial Intelligence, algorithmic decision-making, deepfake technology, synthetic media, or machine-generated evidence. It neither defines AI-generated evidence nor prescribes standards for its authentication, forensic examination, or admissibility.¹²

This legislative silence creates significant uncertainty in the administration of justice. Investigating agencies lack uniform protocols for identifying AI-generated content. Courts remain dependent upon general evidentiary principles developed before the emergence of advanced machine learning technologies. Forensic laboratories continue to face technical limitations in detecting sophisticated deepfakes, while litigants may exploit technological vulnerabilities to fabricate evidence capable of influencing judicial decisions. The absence of statutory safeguards also increases the possibility of wrongful convictions, malicious prosecutions, reputational harm, electoral manipulation, financial fraud, and violations of constitutional rights.¹³

¹² Radha Ranjan, Ankit Kumar, Shagufta Parween, Naveen Nandal, Anupam Sinha, S. Srinivas Kumar & Bhoopathy Rajan, "Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches" in *Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches* (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007.

¹³ R. Sabareesh, Deependra Nath Pathak, Radha Ranjan, Ramachandran Devi Prasanna, P. Shalini & Eijaz Khan Bellary, "AI-Driven Fraud Detection in Banking: Enhancing Transaction Security", 4(3) *Journal of Informatics Education and Research* (2024).

The problem is further compounded by the increasing use of Artificial Intelligence within criminal investigations themselves. Law enforcement agencies worldwide have begun utilizing AI-powered facial recognition systems, predictive policing algorithms, biometric identification technologies, and automated surveillance tools. Although these technologies enhance investigative efficiency, they simultaneously raise concerns regarding algorithmic bias, transparency, accountability, and procedural fairness. Decisions influenced by opaque AI systems may undermine the constitutional guarantees of equality before law, due process, and fair trial.

International jurisdictions have increasingly recognized these challenges by adopting AI-specific regulatory frameworks and digital forensic standards. India's current evidentiary framework, however, continues to rely largely upon principles designed for conventional electronic records rather than sophisticated AI-generated evidence. Consequently, there exists an urgent need to evaluate whether the Bharatiya Sakshya Adhiniyam, 2023 adequately safeguards the integrity of judicial proceedings in the era of Artificial Intelligence.

This research seeks to address this legislative and judicial gap by critically examining the adequacy of the Bharatiya Sakshya Adhiniyam, 2023 in regulating AI-generated evidence, deepfakes, and emerging forms of digital manipulation while balancing technological innovation with constitutional guarantees of fairness and justice.

3. Research Objectives

The present study has been undertaken with the following objectives:

1. To examine the legal framework governing electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023.
2. To analyse the impact of Artificial Intelligence and deepfake technology on the principles of admissibility, authenticity, and reliability of evidence.
3. To evaluate whether the Bharatiya Sakshya Adhiniyam, 2023 adequately addresses the evidentiary challenges posed by AI-generated content.
4. To critically examine the constitutional implications of AI-generated evidence concerning privacy, fair trial, due process, and protection against self-incrimination.
5. To analyse landmark judicial decisions of Indian courts concerning electronic evidence and assess their relevance in the context of Artificial Intelligence.

6. To compare India's legal framework with international approaches adopted in jurisdictions such as the United States, the United Kingdom, Singapore, and the European Union.
7. To identify legislative and procedural deficiencies within the Bharatiya Sakshya Adhiniyam, 2023 concerning AI-generated evidence.
8. To propose legal, institutional, and technological reforms for strengthening India's evidentiary framework in the age of Artificial Intelligence.

4. Research Questions

The study seeks to answer the following research questions:

1. Whether the Bharatiya Sakshya Adhiniyam, 2023 adequately regulates Artificial Intelligence-generated evidence?
2. How does deepfake technology challenge the traditional principles governing admissibility and authentication of electronic evidence?
3. Whether existing provisions relating to electronic records are sufficient to determine the authenticity and reliability of AI-generated content?
4. What constitutional concerns arise from the use of Artificial Intelligence in criminal investigations and judicial proceedings?
5. How have Indian courts interpreted electronic evidence, and are these judicial principles adequate for regulating AI-generated evidence?
6. What lessons can India derive from comparative legal developments concerning Artificial Intelligence and digital evidence?
7. What legislative reforms are necessary to preserve the integrity of judicial proceedings in the era of Artificial Intelligence?

5. Research Hypotheses

The study proceeds on the basis of the following hypotheses:

H₁: The Bharatiya Sakshya Adhiniyam, 2023 modernizes India's law of evidence by recognizing electronic records but does not adequately regulate Artificial Intelligence-generated evidence.

H₂: Deepfake technology significantly undermines the authenticity and reliability of digital evidence, thereby creating substantial risks for criminal and civil adjudication.

6. Research Methodology

The present research adopts a doctrinal and analytical methodology primarily based upon qualitative legal research. The study systematically analyses constitutional provisions, statutory enactments, judicial decisions, governmental reports, scholarly literature, international instruments, and comparative legal frameworks relating to Artificial Intelligence and electronic evidence.

Primary sources include the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, the Constitution of India, the Bharatiya Nagarik Suraksha Sanhita, 2023, relevant rules governing electronic evidence, and landmark decisions of the Supreme Court of India. These statutory materials are critically examined to determine their adequacy in regulating AI-generated evidence.

Secondary sources comprise books, peer-reviewed journal articles, Law Commission reports, governmental publications, parliamentary debates, reports issued by international organizations such as UNESCO, the OECD, the European Commission, and scholarly works concerning Artificial Intelligence, digital forensics, cyber law, constitutional law, and evidence law.

The research further employs a comparative legal approach by examining regulatory frameworks adopted in the United States, the United Kingdom, Singapore, and the European Union. Comparative analysis assists in identifying international best practices capable of informing future legislative reforms in India.

The study also adopts a critical analytical approach, evaluating the interaction between technological innovation and constitutional principles such as privacy, procedural fairness, due process, equality before law, and protection against self-incrimination. The objective is not merely to describe existing legal provisions but to assess their effectiveness in addressing emerging technological realities.

7. Conceptual Framework

7.1 Artificial Intelligence

Artificial Intelligence refers to computational systems capable of simulating human cognitive functions through algorithms designed to learn, reason, predict, and make decisions. Modern

AI systems employ machine learning, deep learning, natural language processing, computer vision, and neural networks to analyse vast quantities of data and generate outputs that increasingly resemble human creativity and intelligence. Unlike traditional software programs that follow predetermined instructions, AI systems continuously improve their performance by learning from data patterns and user interactions.¹⁴

In legal contexts, Artificial Intelligence is increasingly utilized for document review, predictive analytics, legal research, judicial administration, contract drafting, biometric identification, surveillance, forensic analysis, and evidence management. Courts worldwide have begun confronting legal questions concerning algorithmic transparency, accountability, explainability, and the evidentiary reliability of AI-generated outputs.¹⁵

The rapid evolution of Generative Artificial Intelligence represents a significant technological shift. Large Language Models (LLMs), image-generation systems, voice-cloning software, and video synthesis technologies can independently produce content nearly indistinguishable from human-generated material. This capability creates unprecedented opportunities while simultaneously exposing judicial systems to sophisticated forms of digital deception.¹⁶

7.2 Machine Learning and Deep Learning

Machine Learning is a branch of Artificial Intelligence enabling computer systems to improve their performance through experience rather than explicit programming. Algorithms identify patterns within datasets and develop predictive models capable of generating increasingly accurate outputs over time.¹⁷

Deep Learning, a specialized subset of machine learning, utilizes multi-layered artificial neural networks that imitate certain aspects of the human brain. These neural networks process enormous quantities of structured and unstructured data, enabling advanced applications such as facial recognition, autonomous vehicles, language translation, medical diagnostics, and synthetic media generation.

The same technologies that enable beneficial innovation also facilitate sophisticated cybercrimes, identity theft, misinformation campaigns, and the creation of fabricated evidence. Consequently, understanding these technologies is essential for developing effective evidentiary standards under the Bharatiya Sakshya Adhiniyam, 2023.¹⁸

¹⁴ OECD, Artificial Intelligence in Society (OECD Publishing, 2019).

¹⁵ Nils J. Nilsson, The Quest for Artificial Intelligence (Cambridge University Press, 2010).

¹⁶ UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

¹⁷ Information Technology Act, 2000.

¹⁸ Bharatiya Sakshya Adhiniyam, 2023.

8. Deepfake Technology and Synthetic Media: A New Challenge to the Law of Evidence

The exponential growth of Artificial Intelligence has led to the emergence of sophisticated technologies capable of producing synthetic digital content that closely imitates reality. Among these innovations, deepfake technology has emerged as one of the most disruptive developments affecting legal systems worldwide. The term "deepfake" combines "deep learning" and "fake," referring to digitally manipulated audio, video, or images generated through Artificial Intelligence algorithms, particularly Generative Adversarial Networks (GANs). Unlike traditional photo-editing or video manipulation techniques, deepfakes are capable of reproducing an individual's facial expressions, voice, body language, and speech patterns with extraordinary precision, making detection increasingly difficult even for trained observers.¹⁹

Initially developed for academic research in machine learning, deepfake technology has rapidly become accessible through commercial software and open-source platforms. Today, an individual possessing basic technological knowledge can create highly convincing synthetic videos using publicly available AI tools.²⁰ Such democratization of AI-generated content has undoubtedly facilitated creative expression and educational innovation; however, it has simultaneously enabled new forms of cybercrime, fraud, misinformation, electoral manipulation, identity theft, financial deception, revenge pornography, and judicial interference.²¹

From the perspective of evidence law, deepfakes represent a fundamental challenge because the legal system has historically relied upon visual and audio recordings as highly persuasive forms of documentary evidence. Courts have traditionally regarded CCTV footage, video recordings, voice recordings, and digital photographs as objective representations of factual events, provided their authenticity is established. Artificial Intelligence fundamentally disrupts this assumption by enabling the creation of fabricated digital evidence that appears entirely genuine while depicting events that never occurred.²²

¹⁹ OECD, Recommendation of the Council on Artificial Intelligence (2019).

²⁰ Suchi, Shalvi, Arvind Kumar, Anjum Parvez, Radhey Shyam Jha & Deependra Nath Pathak, "Protection of Children from the Evil of Pornography", 6(S1) *International Journal of Health Sciences* 14001–14011 (2022)

²¹ Radha Ranjan & Anupam Sinha, "Child Pornography Laws in India: A Comparative Legal Analysis with Global Frameworks", *The Research Journal (TRJ)*, Vol. 11, Issue 3, May–June 2025, pp. 86–99, ISSN: 2454-7301 (Print), ISSN: 2454-4930 (Online)

²² Chesney, Robert & Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National

The evidentiary implications become particularly significant in criminal trials. A fabricated surveillance recording may falsely place an accused person at the scene of an offence. Similarly, AI-generated voice recordings may falsely suggest confessions, threats, or conspiratorial communications. Deepfake videos may also be used to influence witnesses, intimidate victims, manipulate juries in jurisdictions employing jury trials, or prejudice public opinion through media dissemination before judicial proceedings commence. Consequently, courts can no longer presume that visual evidence inherently reflects objective reality.

The challenges extend equally to civil litigation. Commercial disputes increasingly rely upon electronic communications, video conferences, digital signatures, online contractual negotiations, and electronic documentation. Artificial Intelligence enables malicious actors to manipulate contractual communications, fabricate corporate meetings, or generate false documentary evidence capable of influencing judicial findings concerning liability, consent, or contractual obligations. The economic consequences of such evidentiary manipulation may be substantial, particularly in high-value commercial arbitration and cross-border transactions.

The social implications of deepfake technology have also generated considerable concern. Political leaders have been portrayed delivering fabricated speeches capable of influencing electoral outcomes. Celebrities and private individuals have become victims of non-consensual AI-generated intimate imagery, resulting in severe reputational harm. Financial institutions increasingly encounter AI-generated voice cloning schemes designed to deceive employees into authorizing fraudulent transactions. These developments illustrate that deepfakes no longer represent hypothetical technological risks but constitute practical threats affecting multiple dimensions of governance, commerce, and justice.²³

Legal scholars increasingly argue that evidentiary law must transition from merely recognizing electronic records toward evaluating the technological processes through which such records are created. Traditional authentication principles primarily verify the source of electronic evidence; however, AI-generated evidence requires courts to examine algorithmic processes, training datasets, metadata, model architecture, and forensic indicators capable of revealing synthetic manipulation. Such technical inquiries exceed the conventional expertise of judges and legal practitioners, thereby necessitating greater reliance upon digital forensic experts.

Security" (2019) 107 California Law Review 1753.

²³ Nils J. Nilsson, *The Quest for Artificial Intelligence* (Cambridge University Press, 2010).

Moreover, Artificial Intelligence continuously evolves through machine learning. Consequently, deepfake detection technologies often struggle to identify newly developed synthetic media because detection algorithms typically remain reactive rather than predictive. This technological "arms race" between AI-generated fabrication and forensic detection presents an ongoing challenge for judicial systems seeking to preserve evidentiary integrity.

The Bharatiya Sakshya Adhiniyam, 2023, while recognizing electronic records as documentary evidence, does not expressly distinguish authentic electronic evidence from AI-generated synthetic media. This legislative omission creates uncertainty regarding the evidentiary standards applicable to deepfake content and underscores the necessity for statutory reforms specifically addressing AI-generated evidence.

9. Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

One of the principal objectives underlying the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) was the modernization of India's law of evidence in response to the rapid digitization of society. Unlike the Indian Evidence Act, 1872, which was enacted during the colonial period and subsequently amended to accommodate electronic records, the Bharatiya Sakshya Adhiniyam has been drafted with the explicit recognition that digital evidence now constitutes an indispensable component of judicial proceedings.

The Act substantially retains the conceptual foundations of the earlier Evidence Act while reorganizing and modernizing several provisions. Significantly, the legislation expressly recognizes electronic and digital records as documentary evidence, thereby eliminating many interpretative uncertainties that previously arose under the Indian Evidence Act. Electronic communications, cloud-based documents, computer-generated records, emails, text messages, CCTV footage, metadata, server logs, blockchain records, and digital signatures now clearly fall within the statutory definition of documentary evidence.

The increasing reliance upon digital evidence reflects broader societal transformation. Government services, banking transactions, healthcare administration, educational institutions, commercial contracts, taxation, law enforcement, and judicial administration increasingly operate through digital platforms. Consequently, disputes arising before courts inevitably involve electronic records requiring judicial evaluation. The Bharatiya Sakshya Adhiniyam acknowledges this practical reality by integrating electronic records into the mainstream

evidentiary framework.

However, although the Act modernizes the definition of documentary evidence, its provisions continue to focus primarily upon conventional electronic records rather than Artificial Intelligence-generated content. The legislation does not define "synthetic media," "algorithmically generated evidence," "machine-generated documents," or "deepfake recordings." Consequently, AI-generated evidence must presently be assessed through statutory provisions originally intended for traditional electronic documents rather than autonomous computational outputs.

An important feature of the BSA is its recognition of electronic records produced through modern communication technologies. Electronic contracts, digital certificates, online communications, encrypted records, and digitally signed documents are accorded legal recognition, reflecting India's continued commitment to digital governance. Nevertheless, questions concerning AI-generated authenticity remain unresolved. For example, if an AI system independently generates contractual correspondence based upon machine learning algorithms, should such communication receive the same evidentiary treatment as correspondence authored directly by a human being? The Act presently provides no explicit answer.

Another significant challenge concerns the authentication of AI-generated evidence. Conventional electronic evidence ordinarily requires proof concerning its source, integrity, and chain of custody. AI-generated evidence, however, requires additional verification concerning the computational model that produced the output, the data upon which it was trained, the possibility of algorithmic manipulation, and the reliability of automated decision-making processes. These issues extend beyond traditional evidentiary concepts and require specialized technical expertise.

The BSA also preserves provisions governing the admissibility of electronic records through certification requirements broadly corresponding to the former Section 65B of the Indian Evidence Act. Judicial decisions interpreting these certification requirements remain relevant under the new legislation because they continue to emphasize authenticity, reliability, and procedural safeguards designed to prevent fabrication of electronic evidence.²⁴ However,

²⁴ Russell Stuart & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

certification by itself cannot establish whether sophisticated AI-generated content has been manipulated through deep learning algorithms.

Consequently, although the Bharatiya Sakshya Adhiniyam represents substantial legislative progress toward digital modernization, it does not comprehensively address the unique evidentiary characteristics of Artificial Intelligence-generated evidence. Future judicial interpretation and legislative amendment will therefore play a decisive role in determining the extent to which India's evidentiary framework remains capable of addressing emerging technological challenges.

10. Admissibility, Authenticity, and Reliability of AI-Generated Evidence

The admissibility of evidence constitutes one of the foundational principles governing judicial adjudication. Evidence presented before a court must satisfy legal standards relating to relevance, admissibility, authenticity, and reliability before it can influence judicial determination. These principles have traditionally evolved in relation to human-generated documents, oral testimony, and conventional electronic records. Artificial Intelligence fundamentally complicates this framework because AI-generated evidence may possess convincing authenticity while lacking factual truth.²⁵

Admissibility refers to the legal acceptability of evidence before a court. Under the Bharatiya Sakshya Adhiniyam, electronic records are generally admissible provided statutory requirements concerning authenticity and procedural compliance are satisfied. Yet admissibility alone does not guarantee reliability. A deepfake video may satisfy technical admissibility requirements while nevertheless depicting entirely fabricated events. Therefore, courts must increasingly distinguish between formal admissibility and substantive trustworthiness.²⁶

Authenticity concerns whether evidence genuinely originates from the source it purports to represent. In conventional electronic evidence, authenticity may be established through metadata, digital signatures, hash values, server logs, expert testimony, and chain-of-custody documentation. AI-generated evidence, however, may imitate each of these indicators while

²⁵ Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* (MIT Press 2016).

²⁶ Chesney, Robert & Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security" (2019) 107 California Law Review 1753.

simultaneously concealing algorithmic fabrication. Consequently, traditional authentication mechanisms become insufficient when confronting sophisticated synthetic media.²⁷

Reliability represents an equally significant concern. AI systems frequently operate as "black boxes," meaning that even developers cannot fully explain how particular outputs are generated. Judicial reliance upon evidence produced by opaque computational systems raises fundamental questions concerning procedural fairness and transparency. Courts cannot simply presume that algorithmic outputs possess inherent neutrality because AI systems may reflect biases embedded within their training datasets or programming architecture.

These concerns become particularly acute in criminal prosecutions where the liberty of the accused depends upon evidentiary accuracy. The constitutional presumption of innocence requires that criminal convictions be based upon evidence whose authenticity and reliability have been established beyond reasonable doubt. If AI-generated evidence cannot be adequately verified, excessive judicial reliance upon such material risks wrongful convictions and undermines public confidence in the administration of justice.²⁸

Therefore, the law governing evidence must evolve beyond conventional notions of electronic admissibility and incorporate AI-specific safeguards, including mandatory forensic verification, algorithmic transparency, expert certification, and standardized authentication protocols capable of preserving judicial confidence in digital evidence.²⁹

11. Judicial Approach towards Electronic Evidence in India: Foundations for AI-Generated Evidence

The Indian judiciary has played a pivotal role in shaping the legal principles governing electronic evidence. Although most landmark decisions were rendered under the Indian Evidence Act, 1872, their interpretative value remains highly relevant because the Bharatiya Sakshya Adhiniyam, 2023 substantially retains the evidentiary framework concerning electronic records. Judicial precedents have consistently emphasized that the admissibility of electronic evidence depends not only upon its relevance but also upon its authenticity, integrity, and procedural reliability. These principles assume even greater importance in the era of

²⁷ Ronald J. Allen, *Evidence: Text, Problems and Cases* (Aspen Publishers, 2022).

²⁸ National Institute of Standards and Technology (NIST), *AI Risk Management Framework* (2023).

²⁹ UNESCO, *Guidance for the Governance of Digital Platforms* (2023).

Artificial Intelligence, where digital manipulation has become increasingly sophisticated.

One of the earliest judicial acknowledgements of electronic evidence occurred in *State (NCT of Delhi) v. Navjot Sandhu* (the Parliament Attack Case), where the Supreme Court adopted a liberal approach toward the admissibility of electronic records. The Court held that even in the absence of a statutory certificate under Section 65B of the Indian Evidence Act, electronic evidence could, in certain circumstances, be admitted through other provisions relating to secondary evidence.³⁰ Although this judgment facilitated the reception of electronic evidence, it also generated considerable uncertainty regarding the procedural safeguards necessary to ensure evidentiary reliability.

The uncertainty was resolved by the Supreme Court in *Anvar P.V. v. P.K. Basheer*, where a three-judge Bench overruled *Navjot Sandhu* and held that electronic records constitute a distinct category of evidence requiring strict compliance with the statutory certification requirement. The Court observed that electronic records are inherently susceptible to alteration, duplication, and manipulation. Consequently, documentary safeguards become indispensable for maintaining the integrity of judicial proceedings. The judgment emphasized that the admissibility of electronic evidence cannot be divorced from its authenticity and reliability, thereby recognizing the unique vulnerabilities associated with digital information.³¹

The decision in *Anvar P.V.* represented a watershed moment in Indian evidence law because it acknowledged that technological characteristics necessitate corresponding procedural safeguards. Although the judgment did not specifically contemplate Artificial Intelligence or deepfake technology, its underlying rationale remains directly applicable. If conventional electronic records require statutory authentication because of their susceptibility to alteration, AI-generated evidence—which may be fabricated without detectable traces—requires even more rigorous standards of verification.

Subsequently, conflicting judicial interpretations concerning the mandatory nature of the certificate requirement prompted further clarification by the Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. A three-judge Bench reaffirmed the principles laid down in *Anvar P.V.* and held that the statutory certificate is ordinarily mandatory wherever

³⁰ *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

³¹ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

electronic evidence is sought to be admitted. The Court further clarified exceptional circumstances where production of the certificate may become impossible because the electronic device remains beyond the control of the party seeking to rely upon the evidence.³²

The significance of *Arjun Panditrao* extends beyond procedural compliance. The judgment repeatedly emphasized the necessity of preserving the integrity of electronic evidence throughout its lifecycle—from collection and storage to production before judicial authorities. Such observations acquire greater significance in relation to Artificial Intelligence because AI-generated content can be modified continuously without visibly affecting metadata or digital appearance. Consequently, conventional certification alone cannot adequately establish that digital content has not been algorithmically manipulated.

The Supreme Court's decision in *Tomaso Bruno v. State of Uttar Pradesh* also contributed significantly to the development of electronic evidence jurisprudence. The Court recognized that scientific and technological evidence occupies an increasingly central position within modern criminal investigations. Failure to collect available electronic evidence, including CCTV footage and other digital records, may adversely affect the fairness of criminal proceedings.³³ Although the judgment primarily concerned investigative obligations, it reflects judicial recognition that digital evidence has become indispensable for discovering truth within criminal adjudication.

The constitutional dimensions of technological evidence received comprehensive consideration in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, wherein a nine-judge Bench unanimously recognized the right to privacy as an intrinsic component of Article 21 of the Constitution. The Court observed that technological advancements have fundamentally altered the relationship between individuals and the State by enabling unprecedented forms of surveillance, data collection, and informational profiling.³⁴

Although *Puttaswamy* primarily addressed informational privacy rather than evidentiary law, its principles possess profound implications for Artificial Intelligence. AI-powered surveillance systems, facial recognition technologies, biometric databases, and predictive

³² *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

³³ *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.

³⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

policing algorithms all involve extensive processing of personal data. Where evidence is generated through such technologies, courts must ensure that constitutional guarantees concerning privacy, proportionality, procedural fairness, and legality remain fully respected.

Collectively, these judicial decisions establish three foundational principles that continue to govern electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023. First, electronic evidence requires reliable authentication before judicial reliance can be placed upon it. Secondly, procedural safeguards are indispensable for preserving evidentiary integrity. Thirdly, technological innovation cannot dilute constitutional guarantees protecting individual liberty and fair trial.

Nevertheless, these precedents were developed in an era when Artificial Intelligence had not yet achieved its present sophistication. None of these judgments directly addresses autonomous AI-generated evidence, deepfake videos, voice cloning, synthetic documents, or algorithmically generated visual material. Consequently, while existing jurisprudence provides valuable doctrinal foundations, significant judicial and legislative development remains necessary to address contemporary technological realities.

12. Constitutional Dimensions of Artificial Intelligence and Deepfake Evidence

The admissibility of AI-generated evidence cannot be examined solely through the framework of statutory evidence law. The Constitution of India establishes substantive limitations upon the methods through which evidence may be collected, generated, and utilized within judicial proceedings. Consequently, any evaluation of Artificial Intelligence under the Bharatiya Sakshya Adhiniyam must also consider the constitutional guarantees embodied in Articles 14, 20, and 21.³⁵

12.1 Right to Privacy

The constitutional recognition of privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India significantly transformed the legal relationship between technological innovation and individual liberty. The Supreme Court held that informational privacy forms an essential component of personal autonomy and human dignity. In the digital age, individuals

³⁵ Constitution of India, arts. 14, 20(3), and 21.

continuously generate personal data through online communications, financial transactions, biometric identification, geolocation services, healthcare records, and social media interactions. Artificial Intelligence derives its effectiveness precisely from analysing these extensive datasets.³⁶

AI-powered surveillance systems increasingly rely upon facial recognition, behavioural analytics, predictive algorithms, and biometric verification. While such technologies may enhance law enforcement efficiency, indiscriminate deployment risks creating pervasive systems of digital surveillance inconsistent with constitutional guarantees of privacy. Evidence obtained through AI-driven mass surveillance without adequate statutory safeguards may therefore violate the constitutional requirement that restrictions upon privacy satisfy legality, necessity, proportionality, and procedural fairness.³⁷

Deepfake technology presents an additional privacy concern. Artificial Intelligence enables malicious actors to generate fabricated intimate images or videos using publicly available photographs without the consent or knowledge of the affected individual. Such synthetic media profoundly infringes informational privacy, personal dignity, and reputational interests protected under Article 21.

12.2 Right to Fair Trial

The constitutional guarantee of a fair trial constitutes one of the most fundamental principles governing criminal justice. Fair trial encompasses procedural equality, judicial impartiality, evidentiary reliability, and the opportunity to effectively challenge adverse evidence.

Artificial Intelligence introduces significant challenges to these principles because many advanced AI systems operate as opaque computational models often described as "black boxes." Where judicial decisions depend upon algorithmically generated evidence whose internal reasoning cannot be meaningfully explained, the accused may be deprived of the opportunity to effectively challenge its reliability. Procedural fairness requires that parties understand the evidentiary basis upon which judicial determinations are made. AI systems lacking explainability therefore raise serious constitutional concerns.³⁸

Moreover, algorithmic bias remains a significant issue. Machine learning models derive their predictive capabilities from historical datasets that may themselves reflect social inequalities

³⁶ Radha Ranjan, "Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India", 10(1) *Indian Journal of Law and Human Behavior* 31, 31–38 (2024).

³⁷ UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

³⁸ Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008).

or discriminatory patterns. Judicial reliance upon biased AI-generated evidence risks perpetuating systemic discrimination contrary to Article 14's guarantee of equality before law.

12.3 Protection against Self-Incrimination

Article 20(3) provides that no person accused of an offence shall be compelled to be a witness against himself. Contemporary technological developments raise complex constitutional questions concerning compelled access to digital devices.

Modern smartphones contain enormous quantities of personal information, including communications, photographs, financial records, biometric identifiers, and location histories. Artificial Intelligence enhances investigative capacity by analysing such information to reconstruct behavioural patterns and generate predictive conclusions.

A significant constitutional question arises where investigating agencies compel individuals to provide biometric authentication, facial recognition access, or passwords enabling AI-powered analysis of personal devices. While Indian jurisprudence distinguishes between testimonial and physical evidence, AI's ability to derive extensive personal information from seemingly neutral biometric data complicates this distinction. Future judicial interpretation may therefore require reconsideration of traditional constitutional doctrines in light of technological developments.³⁹

13. Comparative Legal Perspectives on Artificial Intelligence and Digital Evidence

The rapid proliferation of Artificial Intelligence has compelled legal systems across the world to reconsider traditional evidentiary doctrines. Although no jurisdiction has yet developed a completely comprehensive framework governing AI-generated evidence, several countries have introduced legislative measures, judicial guidelines, and regulatory standards that provide valuable lessons for India. A comparative analysis demonstrates that modern legal systems increasingly recognize that conventional evidentiary rules are insufficient for addressing the unique characteristics of Artificial Intelligence, particularly deepfakes, synthetic media, algorithmic decision-making, and machine-generated evidence.

13.1 European Union

Among contemporary legal systems, the European Union has adopted the most comprehensive

³⁹ Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Transparent, Explainable and Accountable AI" (2017) Science Robotics.

regulatory framework for Artificial Intelligence through the Artificial Intelligence Act (AI Act), 2024. Unlike traditional legislation focusing exclusively upon liability or criminal sanctions, the AI Act adopts a risk-based regulatory approach, classifying AI systems into unacceptable-risk, high-risk, limited-risk, and minimal-risk categories. This classification determines the extent of regulatory obligations imposed upon developers, deployers, and users of AI technologies.⁴⁰

The AI Act assumes particular relevance for evidentiary law because several AI systems employed within law enforcement, border control, biometric identification, judicial administration, and criminal investigations fall within the category of high-risk AI systems. Such systems are subject to stringent obligations concerning transparency, human oversight, technical robustness, cybersecurity, record keeping, explainability, and post-market monitoring. Developers are required to maintain comprehensive technical documentation enabling competent authorities to examine the functioning of AI systems whenever disputes arise.⁴¹

The European framework implicitly recognizes that evidentiary reliability depends not merely upon the final digital output but also upon the integrity of the technological processes producing that output. This represents a significant conceptual shift from traditional evidence law, which primarily examines the admissibility of documents rather than the architecture of computational systems generating those documents.

The European Union has also enacted the Digital Services Act and strengthened data protection through the General Data Protection Regulation (GDPR). Together, these instruments establish comprehensive safeguards concerning transparency, accountability, automated decision-making, and protection of personal information. Judicial authorities evaluating AI-generated evidence therefore operate within a broader regulatory ecosystem designed to ensure technological accountability.⁴²

For India, the European approach demonstrates that regulation of Artificial Intelligence cannot be confined exclusively to evidentiary legislation. Instead, evidence law must function alongside broader statutory mechanisms governing AI governance, algorithmic accountability,

⁴⁰ European Parliament and Council, Regulation (EU) 2024/1689 (Artificial Intelligence Act).

⁴¹ Radha Ranjan & Jayini Bhaumik, "Regulating Artificial Intelligence in Legal Practice: An Accountability Framework" in *Blockchain and AI in Business: Applications, Research and Insights* (Gyanavi Publishers & Distributors, 2024). available at: https://www.researchgate.net/publication/383869960_Regulating_Artificial_Intelligence_in_Legal_Practice_An_Accountability_Framework

⁴² European Commission, White Paper on Artificial Intelligence (2020).

cybersecurity, and data protection.⁴³

13.2 United States

The United States has adopted a comparatively decentralized approach towards Artificial Intelligence regulation. Rather than enacting comprehensive federal legislation governing AI-generated evidence, individual states have introduced laws addressing specific manifestations of deepfake technology.

Several states, including California, Texas, Virginia, and New York, have enacted legislation criminalizing malicious dissemination of politically deceptive deepfakes, non-consensual intimate synthetic media, and fraudulent AI-generated communications. These enactments primarily seek to protect electoral integrity, individual privacy, and commercial transactions from technological manipulation.

American courts continue to evaluate AI-generated evidence through traditional evidentiary principles embodied in the Federal Rules of Evidence, particularly rules concerning relevance, authenticity, expert testimony, and scientific reliability. The Daubert standard, developed by the United States Supreme Court, requires scientific evidence to satisfy criteria relating to testing, peer review, error rates, and general acceptance within the relevant scientific community.⁴⁴

Although originally developed for forensic science, the Daubert framework increasingly influences judicial evaluation of algorithmic evidence and AI-generated material. Courts have begun examining whether machine learning models satisfy standards of reliability, reproducibility, and expert validation before admitting computational evidence during litigation.

Recent federal initiatives have also emphasized responsible AI development. The Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (2023) directs federal agencies to develop standards concerning AI safety, watermarking of AI-generated content, cybersecurity, and responsible deployment of generative AI technologies. Although these measures do not directly regulate evidentiary law, they reflect growing governmental recognition that synthetic media presents substantial risks for legal institutions.

⁴³ R. Sabareesh, Deependra Nath Pathak, Radha Ranjan, Ramachandran Devi Prasanna, P. Shalini & Eijaz Khan Bellary, "AI-Driven Fraud Detection in Banking: Enhancing Transaction Security", 4(3) *Journal of Informatics Education and Research* (2024).

⁴⁴ Executive Order No. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (United States, 2023).

13.3 United Kingdom

The United Kingdom has preferred a principles-based regulatory model, relying upon existing legal institutions while gradually developing sector-specific guidance concerning Artificial Intelligence.

The Law Commission of England and Wales has examined numerous legal questions concerning digital evidence, electronic documents, smart contracts, and emerging technologies. British courts continue applying established principles concerning authenticity, chain of custody, and expert evidence while recognizing the increasing complexity of AI-generated digital material.⁴⁵

The Forensic Science Regulator's Code of Practice establishes detailed standards governing collection, preservation, examination, and presentation of digital forensic evidence. These standards emphasize reproducibility, quality assurance, accreditation of forensic laboratories, and transparency concerning analytical methodologies. Such procedural safeguards assume increasing significance where digital evidence may have been manipulated through Artificial Intelligence.⁴⁶

Unlike many jurisdictions, British legal policy strongly emphasizes human oversight. Governmental AI policy repeatedly stresses that automated systems should assist rather than replace human decision-making within judicial and law enforcement contexts. This approach reflects recognition that judicial legitimacy ultimately depends upon accountable human reasoning rather than opaque computational outputs.⁴⁷

13.4 Singapore

Singapore represents one of Asia's most technologically advanced jurisdictions concerning digital governance and evidentiary law.⁴⁸ The Singapore Evidence Act recognizes electronic records while maintaining detailed statutory provisions concerning their authentication and admissibility.

The judiciary has actively promoted digital transformation through electronic filing systems, online dispute resolution, and technologically sophisticated judicial administration. Simultaneously, Singapore has invested substantially in digital forensic capabilities, enabling

⁴⁵ Law Commission of England and Wales, Digital Assets Consultation Paper (2022).

⁴⁶ Forensic Science Regulator, Code of Practice (United Kingdom, 2023).

⁴⁷ UK Government, A Pro-Innovation Approach to AI Regulation (2023).

⁴⁸ R. Ranjan, "Navigating the Digital Frontier: The Intersection of Technology and Criminal Liability in Modern Jurisprudence" in Abhijit B. & Sajal Sharma (eds.), *Disruptive Technologies and the Law: Navigating Legal Challenges in an Era of Innovation* 41, 41–48 (Iterative International Publishers (IIP), 2024).

investigators to detect manipulation of electronic records with greater technical precision.⁴⁹

The Model AI Governance Framework, issued by the Singapore Government, establishes principles concerning explainability, transparency, accountability, and human-centric deployment of Artificial Intelligence. Although primarily intended for commercial AI systems, these principles possess direct relevance for judicial use of algorithmic evidence.

Singapore's approach illustrates that effective regulation requires simultaneous investment in technological expertise, institutional capacity, judicial training, and forensic infrastructure. Legislative reform alone cannot adequately address AI-generated evidence unless supported by corresponding institutional modernization.

14. Legislative Gaps under the Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 undoubtedly represents a progressive step towards modernization of India's law of evidence. Nevertheless, when evaluated against contemporary developments in Artificial Intelligence, several significant legislative deficiencies become apparent.

The most fundamental limitation lies in the absence of statutory recognition of Artificial Intelligence-generated evidence. Although the Act expressly recognizes electronic records, it does not distinguish between conventional digital documents and autonomous computational outputs generated through sophisticated machine learning systems. Consequently, AI-generated photographs, videos, voice recordings, and documents continue to be governed through legal principles originally designed for human-generated electronic records.

Secondly, the Act contains no statutory definition of deepfake technology or synthetic media. Legislative silence concerning these concepts creates interpretative uncertainty because courts must determine admissibility without clear statutory guidance concerning authentication, forensic verification, or evidentiary presumptions applicable to AI-generated content.

A further deficiency concerns authentication standard. Traditional electronic evidence primarily requires proof concerning source, integrity, and chain of custody. AI-generated evidence, however, requires additional examination of algorithmic architecture, training datasets, computational processes, model parameters, metadata integrity, and potential

⁴⁹ Singapore Government, Model Artificial Intelligence Governance Framework (2nd ed., 2020).

adversarial manipulation. The BSA does not prescribe any specialized procedures for such verification.

Another significant concern involves absence of mandatory forensic certification. Presently, electronic evidence may satisfy statutory certification requirements despite having been generated through sophisticated AI manipulation undetectable by conventional technical examination. Without specialized forensic protocols, certification alone cannot adequately establish evidentiary reliability.

The legislation likewise remains silent concerning algorithmic transparency. Judicial evaluation of AI-generated evidence increasingly requires understanding the functioning of computational systems producing particular outputs. Black-box AI systems incapable of meaningful explanation present substantial challenges for procedural fairness because litigants cannot effectively challenge computational reasoning whose internal processes remain inaccessible.

Institutionally, India also faces shortages of digital forensic laboratories, AI specialists, judicial training programmes, and standardized investigative protocols capable of addressing emerging technological challenges. Legislative modernization must therefore be accompanied by corresponding institutional reforms to ensure practical implementation.

Finally, the BSA does not establish any statutory presumption regarding AI-generated evidence, nor does it impose obligations upon parties relying upon such evidence to disclose technological methods used during its creation. Consequently, courts presently lack consistent legal standards for evaluating the credibility of synthetic media.

These deficiencies collectively demonstrate that although the Bharatiya Sakshya Adhiniyam successfully modernizes India's treatment of electronic records, it remains insufficiently equipped to regulate the distinctive evidentiary challenges posed by Artificial Intelligence.

15.Recommendations

The emergence of Artificial Intelligence has fundamentally altered the evidentiary landscape by enabling the creation of highly realistic yet fabricated digital content. While the Bharatiya

Sakshya Adhiniyam, 2023 represents an important legislative milestone in recognizing electronic records as documentary evidence, the analysis undertaken in this study demonstrates that the existing framework remains inadequate to address the unique challenges posed by AI-generated evidence and deepfake technology. To preserve the integrity of judicial proceedings, India must adopt a comprehensive strategy involving legislative reform, judicial capacity building, technological modernization, and international cooperation.

15.1 Statutory Recognition of AI-Generated Evidence

The Bharatiya Sakshya Adhiniyam, 2023 should be amended to expressly define Artificial Intelligence-generated evidence, synthetic media, deepfakes, algorithmically generated records, and machine-generated documents. The absence of statutory definitions creates interpretative uncertainty and leaves courts to apply provisions intended for conventional electronic records to technologically distinct forms of evidence.

A dedicated chapter governing AI-generated evidence would enable Parliament to prescribe specialized rules concerning admissibility, authentication, forensic examination, and evidentiary presumptions.

15.2 Mandatory Digital Forensic Authentication

Every AI-generated photograph, audio recording, video, or document proposed to be relied upon before judicial authorities should undergo mandatory forensic examination by accredited digital forensic laboratories.

Unlike conventional electronic evidence, AI-generated material requires examination of:

- Metadata integrity;
- Algorithmic artefacts;
- Compression inconsistencies;
- Pixel-level manipulation;
- Voice synthesis indicators;
- Neural network signatures;
- Watermark verification; and
- Blockchain-based integrity verification where applicable.

Such forensic authentication should become a statutory prerequisite before AI-generated evidence is admitted during criminal or civil proceedings.

15.3 Establishment of National AI Forensic Laboratories

India presently possesses digital forensic infrastructure; however, specialized expertise concerning Artificial Intelligence remains limited.

The Central Government should establish National Artificial Intelligence Forensic Laboratories equipped with:

- Deepfake detection software;
- Biometric verification systems;
- AI watermark detection tools;
- Synthetic voice analysis technologies;
- Blockchain verification mechanisms;
- Quantum-resistant digital authentication systems.

These laboratories should function independently and provide expert assistance to courts, investigating agencies, and prosecution authorities.

15.4 Judicial Training and Capacity Building

The successful implementation of technologically advanced evidentiary standards depends upon judicial understanding of Artificial Intelligence.

The National Judicial Academy and State Judicial Academies should develop specialized training programmes concerning:

- Artificial Intelligence;
- Machine learning;
- Deepfake technology;
- Digital forensics;
- Algorithmic transparency;
- Electronic evidence;
- Cybersecurity;
- Blockchain technology;
- Biometric authentication.

Continuous judicial education would significantly reduce dependence upon conflicting expert testimony while improving consistency in judicial decision-making.

15.5 Specialized Expert Witness Framework

The Bharatiya Sakshya Adhiniyam should provide statutory recognition for certified AI

forensic experts.

Such experts should possess qualifications in:

- Computer science;
- Artificial intelligence;
- Cyber forensics;
- Digital imaging;
- Machine learning;
- Data analytics.

A national accreditation mechanism should regulate qualifications, ethical obligations, independence, and professional accountability of AI forensic experts appearing before courts.

15.6 Algorithmic Transparency and Explainability

Judicial proceedings must remain transparent and accountable.

Where evidence is generated through Artificial Intelligence systems, parties relying upon such evidence should disclose:

- Algorithmic methodology;
- Source of training data;
- Software version;
- Model architecture;
- Confidence score;
- Probability assessment;
- Limitations of the AI system.

Explainability should become a statutory requirement wherever AI-generated evidence substantially influences judicial findings.

15.7 Chain of Digital Custody

Traditional chain-of-custody principles require significant expansion.

Future legislation should prescribe uniform protocols governing:

- Acquisition of digital evidence;
- Cloud storage;
- Blockchain verification;
- Cryptographic hashing;
- Access logs;

- Audit trails;
- AI processing history.

These safeguards would substantially reduce opportunities for post-collection manipulation.

15.8 International Cooperation

Deepfake dissemination frequently occurs across national borders.

India should actively participate in international cooperation concerning:

- Cybercrime investigations;
- AI governance;
- Digital forensic standards;
- Evidence-sharing mechanisms;
- Mutual legal assistance treaties;
- Harmonization of AI regulations.

Cooperation with organizations such as INTERPOL, the United Nations, the OECD, and the Council of Europe would strengthen India's capacity to investigate transnational AI-enabled offences.

15.9 Ethical Governance of Artificial Intelligence

India should adopt a comprehensive national Artificial Intelligence governance framework emphasizing:

- Fairness;
- Accountability;
- Transparency;
- Explainability;
- Privacy;
- Human oversight;
- Non-discrimination.

Such principles should guide both governmental and private deployment of Artificial Intelligence systems affecting judicial administration.

15.10 Enactment of Comprehensive AI Legislation

Finally, India should consider enacting a dedicated Artificial Intelligence Regulation Act addressing:

- AI governance;
- Liability;
- Civil responsibility;
- Criminal misuse;
- Algorithmic accountability;
- Evidentiary standards;
- Regulatory oversight;
- Ethical obligations.

Such legislation should complement rather than replace the Bharatiya Sakshya Adhiniyam, thereby creating an integrated legal framework capable of responding to future technological developments.

16. Conclusion

Artificial Intelligence represents one of the most transformative technological developments of the twenty-first century. Its applications extend across healthcare, education, finance, governance, transportation, defence, commerce, and judicial administration. Simultaneously, the same technological innovations capable of improving human welfare have generated unprecedented legal challenges, particularly within the law of evidence. Deepfake technology, synthetic media, autonomous content generation, voice cloning, and algorithmic manipulation have fundamentally altered traditional assumptions concerning the authenticity and reliability of documentary evidence.

The Bharatiya Sakshya Adhiniyam, 2023 constitutes a significant legislative achievement by replacing the colonial Indian Evidence Act, 1872 and expressly recognizing electronic records as documentary evidence. The legislation acknowledges India's digital transformation and attempts to modernize evidentiary principles accordingly. Nevertheless, this study demonstrates that recognition of electronic evidence alone is insufficient in an era characterized by rapidly evolving Artificial Intelligence technologies.

The existing statutory framework does not expressly regulate AI-generated evidence, define synthetic media, prescribe forensic standards for deepfake detection, or establish mechanisms ensuring algorithmic transparency. Judicial precedents such as *Anvar P.V.*, *Arjun Panditrao*, and *Puttaswamy* provide valuable doctrinal foundations concerning authenticity, procedural

fairness, and constitutional rights; however, these decisions were developed before the widespread emergence of sophisticated generative Artificial Intelligence.

Comparative analysis reveals that jurisdictions such as the European Union, the United States, the United Kingdom, and Singapore have increasingly recognized the necessity of AI-specific regulatory mechanisms emphasizing transparency, accountability, explainability, human oversight, and technological reliability. India can derive substantial guidance from these developments while designing a legal framework suited to its own constitutional and institutional context.

The future of evidence law must extend beyond traditional concepts of admissibility toward comprehensive regulation of technological processes responsible for generating digital information. Courts can no longer assume that audio recordings, videos, photographs, or electronic documents inherently represent objective reality. Instead, judicial confidence must increasingly depend upon sophisticated forensic verification, algorithmic accountability, and interdisciplinary collaboration between legal institutions and technological experts.

Ultimately, the objective of evidence law remains unchanged: to facilitate the discovery of truth while safeguarding fairness, justice, and constitutional liberty. Artificial Intelligence should strengthen—not undermine—these foundational values. Achieving this objective requires proactive legislative reform, judicial preparedness, technological investment, and ethical governance. If implemented effectively, India can develop a future-ready evidentiary framework capable of preserving both technological innovation and the rule of law in the age of Artificial Intelligence.

Bibliography

- **Books**

1. Allen, Ronald J., Evidence: Text, Problems and Cases (Aspen Publishers, 2022).
2. Goodfellow, Ian, Yoshua Bengio and Aaron Courville, Deep Learning (MIT Press, 2016).
3. Nilsson, Nils J., The Quest for Artificial Intelligence (Cambridge University Press, 2010).

4. Russell, Stuart and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson, 2021).
5. Solove, Daniel J., *Understanding Privacy* (Harvard University Press, 2008).

• **Journal/Articles**

1. Chesney, Robert and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security" (2019) 107 *California Law Review* 1753.
2. Goodfellow, Ian et al., "Generative Adversarial Networks" (2014) *Advances in Neural Information Processing Systems*.
3. Ranjan, Radha, "The Role of Technology in Enhancing the Efficiency of the Bharatiya Nagarik Suraksha Sanhita, 2023" in *Crime and Consequences: A Comprehensive Guide to Criminal Laws in India* (Singhal Law Publications, 2024).
4. Wachter, Sandra, Brent Mittelstadt and Luciano Floridi, "Transparent, Explainable and Accountable AI" (2017) *Science Robotics*.

• **Statutes**

1. Bharatiya Sakshya Adhiniyam, 2023.
2. Bharatiya Nagarik Suraksha Sanhita, 2023.
3. Bharatiya Nyaya Sanhita, 2023.
4. Constitution of India.
5. Information Technology Act, 2000.
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
7. Regulation (EU) 2024/1689 (Artificial Intelligence Act).
8. General Data Protection Regulation (EU) 2016/679.

• **Cases**

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. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
4. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
5. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.

6. Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993).

- **Reports and International Documents**

1. European Commission, White Paper on Artificial Intelligence (2020).
2. Executive Order No. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (United States, 2023).
3. Forensic Science Regulator, Code of Practice (UK, 2023).
4. OECD, AI Principles (2019).
5. OECD, Artificial Intelligence in Society (2019).
6. Singapore Government, Model AI Governance Framework (2020).
7. UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
8. NIST, Artificial Intelligence Risk Management Framework (2023).

