Impact Factor: 9.9 ISSN-L: 2544-980X

Digital Evidence and the Bharatiya Sakshya Adhiniyam: Navigating Admissibility Challenges in the Era of Deepfakes

Dr. Jyoti Rani [1]

Abstract: The rapid evolution of artificial intelligence has introduced deepfake technology as one of the most disruptive challenges to the integrity of digital evidence in modern legal proceedings. India's newly enacted Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaces the Indian Evidence Act of 1872, represents a significant legislative attempt to modernize the evidentiary framework for the digital age. However, questions remain about whether this legislation is adequately equipped to address the admissibility, authentication, and reliability of digital evidence in an era where synthetic media can convincingly fabricate reality. This paper examines the provisions of the BSA related to electronic and digital evidence, evaluates the admissibility challenges posed specifically by deepfake technology, and critically analyses the gap between existing legal standards and the technical sophistication required to adjudicate deepfake-related disputes. Drawing on comparative legal analysis, technical literature, and doctrinal research, this paper argues that while the BSA marks a progressive departure from its colonial predecessor, it requires supplementary statutory guidance, judicial training, and forensic infrastructure to effectively govern deepfake evidence. The paper concludes with policy recommendations for legislative reform and institutional capacity building within India's justice system.

Keywords: Bharatiya Sakshya Adhiniyam, digital evidence, deepfakes, admissibility, artificial intelligence, electronic records, Indian evidence law.

1. Introduction

The admissibility of digital evidence has been a longstanding concern in legal systems across the world. Courts have grappled with questions of authenticity, integrity, and reliability whenever digital records are presented as proof of fact. The challenge has become exponentially more complex with the advent of generative artificial intelligence (AI), particularly deepfake technology, which can produce audio-visual content that is nearly indistinguishable from authentic recordings (Chesney & Citron, 2019). In the context of India's rapidly evolving legal landscape, the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) — replacing the century-and-a-half-old Indian Evidence Act, 1872 — presents both an opportunity and a challenge.

The BSA was enacted as part of the broader criminal law reform initiative alongside the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, together constituting an ambitious overhaul of India's substantive and procedural criminal law architecture. The BSA formally recognizes electronic records and digital documents as admissible evidence, expanding upon the limited framework that existed under Sections 65A and 65B of the Indian Evidence Act (IEA). However, the law's treatment of synthetic or algorithmically generated content, particularly deepfakes, remains conspicuously underdeveloped.

Deepfakes — a portmanteau of "deep learning" and "fake" — are AI-generated synthetic media that manipulate or fabricate a person's likeness, voice, or behavior (Vaccari & Chadwick, 2020). Their increasing accessibility and sophistication have profound implications for legal proceedings: a deepfake video could be used to fabricate confessions, manufacture alibis, create false evidence of crimes, or undermine genuine evidence presented in court. The legal system's ability to detect,

[1] Assistant Professor in Law, Madlauda, Panipat, Haryana

evaluate, and adjudicate disputes involving such material is therefore a matter of pressing public and jurisprudential concern.

This paper proceeds as follows. Section 2 provides a doctrinal analysis of the BSA's provisions concerning digital evidence. Section 3 examines how deepfake technology challenges traditional evidentiary concepts. Section 4 offers a comparative analysis of relevant foreign legal frameworks. Section 5 discusses judicial and forensic institutional capacity. Section 6 presents a critical assessment of the BSA's adequacy and proposes recommendations. Section 7 concludes the paper.

2. Digital Evidence Under the Bharatiya Sakshya Adhiniyam, 2023

2.1 Foundational Provisions and Definitional Scope

The BSA adopts a broad and technologically forward definition of electronic records. Under Section 2(1)(t), the Act defines an "electronic record" to include data, record, or data generated, image, or sound stored, received, or sent in an electronic form or microfilm or computer-generated microfiche. This definition aligns broadly with the Information Technology Act, 2000 (IT Act), which provides the primary definitional framework for electronic records in Indian law (Ministry of Law and Justice, 2023).

Significantly, the BSA expands upon the IEA by explicitly recognizing electronic and digital records as documentary evidence under Section 57. This marks a structural elevation of digital material from a secondary evidentiary category, where it was occasionally subject to contested admissibility, to a primary one. The Act also introduces provisions relating to "electronic or digital records" under Chapter V, codifying their admissibility subject to conditions of authentication and certification.

2.2 The Certification Requirement

One of the most consequential provisions in the BSA's digital evidence framework is the requirement of a certificate of authenticity. Under Section 63 of the BSA — which substantially mirrors and modernizes Section 65B of the IEA — electronic records are admissible only if accompanied by a certificate issued by a responsible official identifying the computer that produced the record, confirming that the computer was in proper working condition, and attesting that the information was produced in the ordinary course of activities (Sharma, 2023).

The Supreme Court of India had previously rendered significant jurisprudence on this requirement through Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), wherein a three-judge bench held that the Section 65B certificate is mandatory and cannot be bypassed even when the original device is produced in court. The BSA codifies this approach, though its application to AI-generated or manipulated content remains legally untested.

The certification framework was designed for a world in which digital records are primarily records of transactions, communications, and human-generated data stored and retrieved by computer systems. It did not anticipate a category of evidence that is itself created by AI with the express intention of mimicking authentic content. The certificate attests to the integrity of the process by which the computer generated or stored the data, but it says nothing about whether the underlying content reflects reality (Reed, 2022). In the case of a deepfake, the computer may have functioned perfectly — and still produced a fabricated recording.

2.3 Best Evidence and Secondary Evidence

The BSA retains the principle that the best available evidence should be produced before the court. Section 56 and its related provisions permit secondary evidence of documents in defined circumstances, including when the original is lost, destroyed, or cannot be produced without undue delay. For electronic records, this principle has been interpreted to mean that printouts and copies are admissible with the certificate, even when the original device is not available (Kataria, 2023).

However, in deepfake disputes, the very concept of an "original" becomes philosophically and technically problematic. A deepfake video may be rendered at a resolution and quality that is technically superior to a genuine recording. It may exist on multiple servers, have multiple copies with

identical metadata, and be mathematically indistinguishable from an authentic file without forensic AI analysis. Traditional legal categories of "original" and "copy" are structurally ill-suited to address this phenomenon.

2.4 Presumption of Electronic Records

Section 81A and related presumptive provisions in the BSA permit courts to presume the accuracy of electronic records under certain conditions, particularly those published in official forms or generated by automated systems. This presumption, while administratively useful, may be dangerously misapplied in cases involving AI-generated content. Courts operating under such a presumption may be inclined to accept digital audio-visual evidence without demanding the level of forensic scrutiny that deepfake detection requires (Nair & Verma, 2022).

3. Deepfake Technology and the Evidentiary Crisis

3.1 Technical Architecture of Deepfakes

Deepfakes are primarily generated using Generative Adversarial Networks (GANs), a class of machine learning models in which two neural networks — a generator and a discriminator — compete against each other to produce increasingly realistic synthetic outputs (Goodfellow et al., 2014). In the context of video manipulation, a deepfake system is trained on a large dataset of images and videos of a target individual, allowing the generator to produce new images of that person performing actions, speaking words, or expressing emotions they never actually exhibited.

More recent developments include diffusion models and transformer-based architectures that produce deepfake content of even higher fidelity and are more resistant to detection than GAN-based outputs (Rombach et al., 2022). The accessibility of open-source deepfake tools has democratized the production of synthetic media, meaning that sophisticated forgeries can now be produced by individuals with modest technical expertise and commercially available hardware.

3.2 Deepfakes as Evidentiary Threats

The legal system faces three primary categories of deepfake-related evidentiary threats. First, deepfakes may be introduced as affirmative false evidence — fabricated recordings of a defendant committing a crime, a witness giving a statement, or a party entering into an agreement. Second, genuine evidence may be challenged as a deepfake, creating reasonable doubt about authentic recordings. This phenomenon, sometimes called the "liar's dividend," allows guilty parties to cast doubt on legitimate evidence by alleging it is AI-generated (Chesney & Citron, 2019). Third, deepfakes may contaminate the broader evidentiary environment by making fact-finders generally skeptical of all digital recordings, undermining the probative value of even unimpeachable evidence.

3.3 Detection Challenges and Limitations

While various technical methods exist for detecting deepfakes — including analysis of facial blinking patterns, inconsistencies in lighting and shadow, spectral analysis of audio frequencies, and digital watermarking — none of these methods offers a universal or definitive solution (Tolosana et al., 2020). Detection accuracy is highly dependent on the quality of the deepfake, the specific algorithm used to generate it, and the sophistication of the detection model applied. Critically, as detection models improve, generative models are refined to evade them, resulting in an ongoing technological arms race with no stable equilibrium.

From a legal standpoint, this means that the reliability of deepfake detection evidence is itself subject to challenge under the same standards of scientific reliability that courts apply to other forms of expert testimony. In India, the admissibility of expert evidence is governed by Section 45 of the IEA (now restructured under Section 39 of the BSA), which permits courts to receive opinions of persons "specially skilled" in a relevant art, science, or trade. Whether deepfake detection meets the threshold of a recognized scientific discipline with established methodologies and error rates is a question that Indian courts have not yet authoritatively resolved.

3.4 Metadata, Hash Values, and Their Limitations

Legal practitioners often rely on metadata and cryptographic hash values as tools for authenticating digital evidence. Hash functions such as SHA-256 generate a unique digital fingerprint for any given file, allowing verification that the file has not been altered after a specific point (Casey, 2011). However, a deepfake video that is created and preserved without subsequent alteration will produce a consistent hash value. The hash certifies only that the file is unmodified from the point at which it was hashed; it says nothing about whether the content is genuine. This is a fundamental limitation that legal practitioners and courts must understand: cryptographic integrity is not the same as substantive authenticity.

4. Comparative Legal Analysis

4.1 The United States

In the United States, digital evidence is primarily governed by the Federal Rules of Evidence (FRE), particularly Rule 901 on authentication, and Rule 702 on expert testimony, which requires that scientific evidence be based on sufficient facts or data, reliable methodology, and appropriate application (Federal Rules of Evidence, 2023). The *Daubert* standard, established in *Daubert v. Merrell Dow Pharmaceuticals* (1993), provides the general framework for courts to assess the reliability of scientific expert testimony, including digital forensics.

Several U.S. states have enacted specific legislation addressing deepfakes in electoral and non-consensual intimate contexts, including California's AB 602 and AB 730 (enacted 2019), and Texas's Senate Bill 751 (2023), which criminalizes the use of deepfake media to influence elections. However, comprehensive federal evidentiary standards specifically addressing deepfake authentication have not yet been enacted (Rini, 2020). The National Institute of Standards and Technology (NIST) has published guidelines on digital evidence integrity, and the Department of Defense's Media Forensics program (MediFor) has funded significant research into automated deepfake detection.

4.2 The European Union

The European Union's approach to AI-generated synthetic media is largely situated within the broader regulatory framework of the EU Artificial Intelligence Act (AIA), adopted in 2024, which classifies certain deepfake applications as high-risk or prohibited AI systems (European Parliament, 2024). The AIA imposes disclosure obligations on developers and deployers of systems that generate synthetic content, requiring that outputs be labeled as AI-generated. This labeling requirement, if implemented effectively, would directly aid evidentiary evaluation by providing a technical marker that courts could identify.

The EU's eIDAS Regulation and the General Data Protection Regulation (GDPR) provide complementary frameworks for the authentication of electronic documents and the protection of biometric data, respectively. Together, these instruments create a more structured legal environment for digital evidence than currently exists in India (Erdos, 2022). The EU model suggests that systemic evidentiary reform requires not only evidence law amendments but also upstream regulation of AI development and deployment.

4.3 The United Kingdom

The United Kingdom's approach to digital evidence has been shaped significantly by the Law Commission's 2022 report on digital evidence, which recommended updating the Police and Criminal Evidence Act 1984 (PACE) framework to address the reliability challenges posed by AI-generated content. The report specifically noted that the traditional presumption of computer reliability — that computer-generated records are accurate unless there is evidence to the contrary — is ill-suited to the deepfake era and recommended a shift toward a more neutral, case-by-case reliability assessment (Law Commission, 2022).

The UK's approach is instructive for India because both legal systems share common law foundations and the Indian Evidence Act was itself modeled on English evidentiary principles. The Law

Commission's recommendation to abandon automatic presumptions of digital reliability and replace them with structured reliability inquiries offers a directly transferable model for BSA reform.

4.4 Singapore

Singapore's Evidence Act permits the admission of computer output in evidence under conditions substantially similar to India's Section 65B framework. However, Singapore has supplemented its evidentiary framework with the Protection from Online Falsehoods and Manipulation Act (POFMA), 2019, and has enacted amendments to the Penal Code addressing deepfake non-consensual intimate imagery (Ministry of Home Affairs Singapore, 2022). Singapore's approach demonstrates that specialized legislation addressing synthetic media can co-exist with a general evidentiary framework, providing targeted legal remedies without requiring wholesale revision of evidence law.

5. Judicial and Forensic Institutional Capacity in India

5.1 Current State of Digital Forensics Infrastructure

India's ability to adjudicate deepfake-related evidentiary disputes is significantly constrained by the current state of its digital forensics infrastructure. The Central Forensic Science Laboratory (CFSL) and state-level forensic science laboratories (FSLs) are responsible for examining digital evidence in criminal proceedings. However, these institutions face substantial resource constraints, technological gaps, and a significant backlog of pending forensic examinations (Rao & Chakrabarti, 2021).

As of the time of writing, no Indian public forensic laboratory has published standardized protocols for deepfake detection or AI-generated media analysis. This absence means that courts receiving deepfake-related evidence have no established institutional reference point for evaluating the reliability of detection methodologies presented by private experts. The resulting evidentiary asymmetry — in which well-resourced parties can retain sophisticated forensic experts while others cannot — raises serious concerns about equality of arms and fair trial rights guaranteed under Article 21 of the Constitution of India.

5.2 Judicial Capacity and Technology Literacy

The effective adjudication of deepfake evidence requires judges to possess, or have access to, sufficient technical literacy to evaluate competing expert claims about AI-generated media. Research on judicial technology literacy in India suggests that while the higher judiciary has shown increasing awareness of technology-related legal issues — particularly in intellectual property, cybercrime, and data protection matters — systematic judicial education in AI and digital forensics remains limited (Srinivasan & Ghosh, 2022).

The Supreme Court's e-Committee has developed various digital initiatives under the National e-Courts Project, and the National Judicial Academy conducts periodic training programs on cyber law and digital evidence. However, training on the specific evidentiary challenges posed by AI-generated content, including deepfakes, has not been systematically incorporated into judicial education curricula. Without such training, courts are poorly equipped to exercise the gatekeeping function that effective deepfake evidence management requires.

5.3 Expert Witness Framework

The BSA's provisions on expert evidence — substantially carrying forward the approach of Section 45 of the IEA — do not prescribe any minimum qualifications or methodological standards for experts in digital forensics or AI. This is in contrast to systems like the U.S. *Daubert* framework or the UK's Criminal Procedure Rules, which impose structured reliability assessments on expert evidence. In practice, this means that courts in India may receive competing expert testimony on deepfake authenticity from witnesses with vastly different levels of qualification and methodological rigor, with limited legal tools to distinguish reliable from unreliable opinions (Baxi, 2020).

6. Critical Assessment and Recommendations

6.1 The BSA's Strengths and Structural Limitations

The BSA represents a genuine and significant improvement upon the IEA's digital evidence framework. Its explicit recognition of electronic and digital records as primary documentary evidence, the consolidation of the certification requirement under Section 63, and the alignment of definitions with the IT Act provide a more coherent foundational framework than previously existed. These are meaningful legislative achievements.

However, the BSA's deepfake-related limitations are structural rather than incidental. The Act was drafted and enacted before deepfake-specific evidentiary challenges had been fully articulated in Indian judicial or legislative discourse. As a result, it applies general digital evidence principles to a category of evidence that requires specialized treatment. The certification framework attests to process integrity but not content authenticity. The presumptions of electronic record accuracy are potentially dangerous when applied to synthetic media. The expert evidence provisions provide no methodological guardrails for deepfake detection testimony (Pandey, 2023).

These are not minor technical gaps that creative statutory interpretation can bridge. They represent a fundamental mismatch between the legal framework and the technological reality it must govern.

6.2 Recommendations for Legislative Reform

First, the BSA should be supplemented by a dedicated provision addressing the admissibility and authentication of AI-generated or potentially AI-generated media. This provision should require that parties seeking to admit audio-visual digital evidence in criminal proceedings certify, to the best of their knowledge, that the evidence has not been generated or materially altered by AI. It should further require that any party challenging digital evidence on deepfake grounds provide a prima facie technical basis for that challenge before the court initiates a reliability inquiry.

Second, the legislature should consider enacting a standalone Digital Evidence Reliability Act or incorporating a structured reliability framework into the BSA through amendment. This framework should specify that courts must conduct a pre-admission reliability inquiry for challenged digital evidence, drawing on specified criteria including the provenance and chain of custody of the evidence, the detection methodology applied, the error rates of the detection method, and the qualifications of the expert witness (Law Commission of India, 2023).

Third, the IT Act should be amended to impose disclosure obligations on developers and deployers of AI systems capable of generating realistic synthetic media. Such systems should be required to embed verifiable provenance metadata — such as C2PA (Coalition for Content Provenance and Authenticity) standard markers — in all outputs. This upstream technical intervention would significantly ease the downstream evidentiary burden by creating a technical trail that courts can examine (Stahl et al., 2023).

6.3 Recommendations for Institutional Capacity Building

The CFSL and state FSLs must be equipped with dedicated AI and synthetic media forensics units staffed by professionals with expertise in machine learning, computer vision, and audio forensics. The central government should allocate dedicated budgetary resources for this purpose and establish a National Digital Forensics Centre with a specific mandate to develop, standardize, and periodically update deepfake detection protocols for use by Indian courts.

The National Judicial Academy should develop a mandatory module on AI-generated evidence for judicial education, covering the technical basics of deepfake generation and detection, the legal standards applicable to expert testimony in this domain, and illustrative case studies from Indian and comparative jurisdictions. High Courts should issue practice directions establishing the procedural framework for deepfake-related evidentiary disputes, including timelines for forensic examination, standards for appointing court experts, and guidelines for evaluating competing expert testimony.

6.4 The Constitutional Dimension

The admissibility of deepfake evidence — or the wrongful exclusion of genuine evidence challenged as a deepfake — has direct constitutional implications. The right to a fair trial under Article 21 of the Constitution of India encompasses the right to present and challenge evidence. If courts lack the tools to reliably distinguish genuine from synthetic digital evidence, both the prosecution's right to rely on authentic digital evidence and the accused's right to challenge fabricated digital evidence are materially compromised.

The Supreme Court's jurisprudence on digital evidence, from *State (NCT of Delhi) v. Navjot Sandhu* (2005) to *Arjun Panditrao* (2020), has consistently emphasized the importance of reliability and authenticity as prerequisites for evidentiary admissibility. The deepfake era requires that this constitutional commitment to reliable evidence be given substantive meaning through adequate legislative, institutional, and judicial mechanisms (Divan & Rosencranz, 2021).

6.5 The Role of International Cooperation

Deepfakes transcend national borders. A deepfake video may be generated on servers in one country, distributed through platforms headquartered in another, and introduced as evidence in courts of a third. Effective legal governance of deepfake evidence therefore requires international cooperation in at least three domains: mutual legal assistance treaties (MLATs) that facilitate cross-border access to digital evidence; harmonized technical standards for synthetic media detection and provenance; and coordinated regulatory approaches to AI disclosure obligations.

India should actively engage with multilateral bodies including the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL), and the G20's Digital Economy Working Group to advance harmonized standards for deepfake evidence governance. India's Presidency of the G20 in 2023 and its active participation in global AI governance discussions provide a meaningful diplomatic platform for this engagement (Ministry of External Affairs, 2023).

7. Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 represents India's most significant modernization of evidentiary law since independence. Its recognition of digital records as primary evidence, its consolidation of the certification requirement, and its alignment with the Information Technology Act provide a more coherent foundation for digital evidence governance than the colonial-era framework it replaces. These achievements deserve recognition.

Yet the BSA was designed for a digital world in which the primary challenge was ensuring the integrity of human-generated electronic records — not for a world in which AI systems can fabricate convincingly realistic recordings of events that never occurred. Deepfake technology exposes fundamental structural limitations in the BSA's approach to digital evidence authentication, its presumptions of electronic record reliability, its expert evidence framework, and its absence of any synthetic media-specific provisions.

The gap between the BSA's framework and the evidentiary challenges of the deepfake era is not merely a legislative gap; it is an institutional one. India's forensic laboratories lack the capacity to conduct reliable deepfake detection. Its judicial education system has not yet systematically integrated AI evidentiary challenges into training curricula. Its expert witness framework provides no methodological guardrails for the reliability of deepfake detection testimony.

Bridging this gap requires a multi-pronged response: legislative amendment to the BSA introducing a structured reliability framework for AI-generated evidence; upstream regulation of synthetic media tools through IT Act amendments requiring provenance metadata; institutional investment in specialized digital forensics capacity; mandatory judicial education on AI evidence; and active international engagement in deepfake governance standard-setting.

The integrity of legal proceedings is foundational to the rule of law. If courts cannot reliably distinguish truth from fabrication in the digital record, the legitimacy of evidence-based adjudication is

at risk. The BSA's architects recognized that Indian evidence law needed to meet the challenges of the digital age. The deepfake era demands that this recognition be translated into legal and institutional mechanisms adequate to the technological moment. India's justice system must now move from acknowledging the challenge to governing it.

References

1. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Supreme Court of India).
2. Baxi, U. (2020). *The future of human rights* (4th ed.). Oxford University Press.
3. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
4. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J
5. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
6. Divan, S., & Rosencranz, A. (2021). *Environmental law and policy in India* (3rd ed.). Oxford University Press.
7. Erdos, D. (2022). GDPR and the European data protection framework: Towards a mature synthesis. *Modern Law Review*, *85*(2), 401–432.
8. European Parliament. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
9. Federal Rules of Evidence. (2023). *Federal Rules of Evidence* (as amended to December 1, 2023). United States Courts. https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_-_december_2023_0.pdf
10. Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, *27*, 2672–2680.
11. Kataria, J. L. (2023). *The Bharatiya Sakshya Adhiniyam with commentary* (1st ed.). Universal Law Publishing.
12. Law Commission. (2022). *Digital evidence: Report on the admissibility and authentication of digital evidence in criminal proceedings* (Law Com No 403). Her Majesty's Stationery Office.
13. Law Commission of India. (2023). *Report on digital evidence and electronic records in the Indian legal system* (Report No. 289). Government of India.
14. Ministry of External Affairs. (2023). *India's G20 presidency: Digital economy priorities*. Government of India. https://www.g20.in/en/g20-india/presidency.html
15. Ministry of Home Affairs Singapore. (2022). *Amendments to the Penal Code (online falsehoods and deepfakes)*. Singapore Government. https://www.mha.gov.sg
16. Ministry of Law and Justice. (2023). *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023). Gazette of India Extraordinary.
17. Nair, R., & Verma, S. (2022). Evidentiary presumptions in the digital age: Rethinking the reliability standard for electronic records in India. *Indian Law Review*, *6*(3), 289–311.
18. Pandey, P. (2023). Reforming India's evidence law for the digital era: An analysis of the Bharatiya Sakshya Adhiniyam. *Journal of Indian Law and Society*, *14*(2), 115–142.

19. Rao, G., & Chakrabarti, A. (2021). Digital forensic capacity in India: Challenges and prospects. *Indian Journal of Criminology and Criminalistics*, *42*(1), 55–78.

20. Reed, C. (2022). *Making laws for cyberspace*. Oxford University Press.

21. Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosopher's Imprint*, *20*(24), 1–16.

22. Rombach, R., Blattmann, A., Lorenz, D., Esser, P., & Ommer, B. (2022). High-resolution image synthesis with latent diffusion models. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 10684–10695. https://doi.org/10.1109/CVPR52688.2022.01042

23. Sharma, R. (2023). Section 63 of the Bharatiya Sakshya Adhiniyam and the digital evidence certification framework. *National Law School of India Review*, *35*(1), 44–68.

24. Srinivasan, P., & Ghosh, A. (2022). Judicial technology literacy and digital adjudication in India: An empirical study. *Asian Journal of Legal Education*, *9*(2), 183–205.

25. Stahl, B., Antoniou, J., Ryan, M., Macnish, K., & Jiya, T. (2023). Organisational responses to the ethical issues of artificial intelligence. *AI & Society*, *38*(1), 23–37. https://doi.org/10.1007/s00146-021-01148-6

26. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (Supreme Court of India).

27. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, *64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

28. Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, *6*(1), 1–13. https://doi.org/10.1177/2056305120903408