



Evidentiary challenges of deepfake sexual offenses: An empirical analysis of judicial responses under India's new criminal law framework

Vishal Anand

Research Scholar, University Department of Law, Patna University, Patna, Bihar, India

DOI: <https://doi.org/10.66856/ijl.2026.12.3.12294>

Abstract

The proliferation of Generative Adversarial Networks (GANs) has precipitated a crisis of visual truth in criminal jurisprudence, particularly concerning technology-facilitated sexual violence. With the transition from the Indian Penal Code (IPC) and Indian Evidence Act (IEA) to the Bharatiya Nyaya Sanhita, 2023 (BNS) and Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Indian legal system faces the unprecedented challenge of prosecuting non-consensual deepfake pornography. This article empirically examines the judicial responses and evidentiary hurdles associated with deepfake sexual offenses under the new criminal framework. While the BNS modernizes offenses – encompassing privacy violations (Section 77), defamation (Section 356), and deceitful sexual conduct – and the BSA elevates electronic records with updated authentication mandates (Section 63), the substantive law remains conceptually strained by synthetic media. Utilizing a mixed-methods approach comprising doctrinal analysis and qualitative assessments of early judicial interventions and cyber-forensic data, this study investigates how trial courts navigate the “Liar’s Dividend” – a phenomenon where the accused weaponizes the existence of deepfakes to cast reasonable doubt on genuine digital evidence. The findings reveal a critical legal gap: Section 63 certifies authenticating the source device or storage media but cannot verify the pixel-level integrity of AI-generated content. Consequently, the reliance on under-resourced forensic laboratories creates severe trial bottlenecks. The paper concludes that without integrating AI-driven forensic verification and specialized digital jurisprudence, the BNS and BSA frameworks risk procedural paralysis, thereby exacerbating victim trauma and undermining the administration of criminal justice.

Keywords: Bharatiya Sakshya Adhiniyam, Deepfake Pornography, Digital Evidence, Generative Adversarial Networks, Liar’s Dividend

Introduction

The integration of Artificial Intelligence (AI) into everyday digital interfaces has fundamentally disrupted the foundational assumptions of criminal law, particularly regarding the authenticity, reliability, and attribution of digital evidence. The most pressing manifestation of this disruption is the “deepfake” – hyper-realistic synthetic media created using machine learning techniques to manipulate or fabricate visual and audio content ^[1]. In India, the weaponization of deepfakes has increasingly taken a gendered dimension, manifesting as non-consensual deepfake pornography and technology-facilitated sexual offenses. This algorithmic manipulation not only constitutes a severe violation of bodily autonomy and privacy (Article 21 of the Constitution of India) but also introduces acute evidentiary complexities in the courtroom.

On July 1, 2024, India’s criminal justice system underwent a paradigm shift with the enforcement of the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Sakshya Adhiniyam (BSA), replacing the colonial-era IPC and IEA ^[2]. While the BSA expressly acknowledges electronic records and attempts to streamline their admissibility under Section 63 (the successor to Section 65B of the IEA), the forensic reality of deepfakes challenges the traditional legal binaries of primary and secondary evidence. When synthetic media is nearly indistinguishable from reality, establishing the *actus reus* (the act of algorithmic creation/dissemination) and *mens rea* (criminal intent) under the BNS requires a level of technological literacy and forensic infrastructure that trial courts are currently struggling to operationalize.

Review of Literature

Scholarly discourse surrounding deepfakes in India has predominantly focused on intermediary liability, electoral integrity, and personality rights, with limited empirical focus on criminal trial mechanics. Academic evaluations of the Information Technology Act, 2000 (specifically Sections 66E, 67, and 67A) highlight the statute’s inability to distinguish between physically captured obscenity and algorithmically generated synthetic imagery ^[3]. Recent analyses of the BSA, 2023, note that while the Act retains a technology-neutral approach to electronic records, it fails to provide specialized statutory presumptions for AI-manipulated evidence ^[4]. Legal scholars have increasingly invoked the concept of the “Liar’s Dividend,” arguing that the mere existence of deepfake technology allows perpetrators to inject doubt into proceedings by falsely claiming that genuine incriminating digital evidence is a deepfake ^[5]. However, the literature remains largely theoretical, lacking ground-level empirical data on how Indian trial court judges and cyber cells are practically applying the new BNS/BSA provisions to these novel offenses.

Research Gap

Despite the profound implications of synthetic media, there is a distinct lack of socio-legal empirical research examining the intersection of deepfake sexual offenses and the newly implemented BNS and BSA frameworks. Existing studies predate the July 2024 legislative overhaul and rely on the repealed IPC and IEA. Specifically, there is an absence of empirical data mapping the judicial capacity of trial courts

to evaluate Section 63 BSA certificates when the integrity of the electronic record (not just the custody of the device) is contested due to suspected AI manipulation.

Research Questions

To address the identified gaps, this study is guided by the following research questions:

1. How do trial courts and investigative agencies empirically assess the authenticity and admissibility of electronic records involving alleged deepfake sexual offenses under Section 63 of the BSA?
2. What are the primary evidentiary and doctrinal hurdles in establishing *mens rea* and *actus reus* for deepfake-facilitated sexual violence under the applicable sections of the BNS and IT Act?

Hypotheses

1. **H1:** The procedural safeguards for electronic evidence under Section 63 of the BSA are insufficient to independently authenticate hyper-realistic deepfakes without specialized forensic expert testimony, leading to prolonged trial delays and lower conviction rates.
2. **H2:** The absence of a *sui generis* offense for synthetic sexual media in the BNS forces judicial reliance on fragmented provisions (such as defamation and obscenity), which fail to capture the unique algorithmic harm of deepfakes, thereby allowing the accused to successfully leverage the “Liar’s Dividend.”

Research Methodology

This study adopts a mixed-methods socio-legal research design, integrating doctrinal legal research with qualitative empirical methodology. The doctrinal component critically analyzes the statutory text of the BNS, 2023, the BSA, 2023, the Digital Personal Data Protection Act (DPDPA), 2023, and the IT Act, 2000, alongside evolving judicial precedents (e.g., High Court John Doe injunctions regarding personality rights). The empirical component utilizes a phenomenological approach to understand the lived experiences and practical challenges of the primary stakeholders in the criminal justice system.

Data Collection

1. **Primary Data:** Qualitative data collected through structured, in-depth interviews and case-file analysis. The sample includes (a) Cyber-cell investigating officers dealing with digital forensics, (b) Public prosecutors handling technology-facilitated sexual offenses, and (c) Independent digital forensic experts accredited by the Ministry of Electronics and Information Technology (MeitY).
2. **Secondary Data:** Statutory laws, parliamentary committee reports on the new criminal bills, National Crime Records Bureau (NCRB) data on cybercrimes, and published appellate court judgments concerning electronic evidence.

Scope and Limitations

The scope of this research is strictly confined to non-consensual deepfake pornography and technology-facilitated sexual offenses within the jurisdiction of Indian criminal law. It evaluates the legal landscape post-July 1,

2024, focusing exclusively on the BNS and BSA. The primary limitation of this study is the nascent stage of BNS/BSA jurisprudence; as the laws have been recently enacted, trial court judgments leading to final convictions under these specific statutes are still emerging, necessitating a reliance on interlocutory orders, cyber-cell investigation patterns, and expert legal consensus.

The Substantive Void: Mapping Deepfake Harms against the BNS and IT Act

1. Introduction to the Ontological Shift in Digital Offenses

The fundamental premise of traditional criminal law relies on a direct causal nexus between the physical act of the perpetrator (*actus reus*) and the physical or psychological harm suffered by the victim. However, the emergence of Generative Adversarial Networks (GANs) and deepfake technology has created an ontological shift in how sexual offenses are perpetrated in the digital sphere. Synthetic media divorces the victim’s physical body from the sexually explicit content, superimposing their biometric identity (face or voice) onto a fabricated scenario ^[6]. This chapter critically evaluates whether the Bharatiya Nyaya Sanhita, 2023 (BNS), working in conjunction with the Information Technology Act, 2000 (IT Act), possesses the statutory elasticity to adequately criminalize this novel form of technology-facilitated sexual violence, or if it leaves a critical substantive void.

2. The Limitations of Section 77 BNS (Voyeurism) and Privacy Violations

Under the erstwhile Indian Penal Code (IPC), Section 354C addressed voyeurism. The BNS modernizes this under Section 77, criminalizing the act of a man watching or capturing the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed ^[7].

From an empirical and doctrinal standpoint, applying Section 77 to deepfakes presents an insurmountable hurdle regarding the *actus reus*. Deepfake pornography does not involve “capturing” an image of the victim engaging in a private act; rather, it involves harvesting public or benign images (e.g., from social media) and algorithmically fabricating a private, sexualized act that never physically occurred. Because penal statutes are subject to the rule of strict interpretation, trial courts cannot extend the definition of “capturing” to mean “fabricating through artificial intelligence.” Consequently, an analysis of preliminary cyber-crime FIRs registered post-July 2024 indicates that defense counsels frequently succeed in getting Section 77 charges quashed at the framing stage when the imagery is demonstrably synthetic ^[8].

3. Outraging Modesty (Section 74 BNS) and Defamation (Section 356 BNS)

In the absence of a *sui generis* provision for non-consensual synthetic media, investigating agencies often default to Section 74 of the BNS (assault or use of criminal force to woman with intent to outrage her modesty) or Section 356 (defamation).

While Section 74 aims to protect the dignity of women, its historical jurisprudence is rooted in physical proximity and the application of “criminal force” or “assault.” Expanding “criminal force” to encompass the dissemination of

deepfakes requires judicial acrobatics that higher courts are largely reluctant to perform^[9].

Alternatively, prosecuting deepfakes under Section 356 BNS (defamation) severely dilutes the gravity of the offense. Classifying non-consensual deepfake pornography merely as an injury to “reputation” completely ignores the profound, gendered trauma and violation of bodily autonomy inherent in the act. Defamation also allows for exceptions such as “truth for public good,” which, while inapplicable to fabricated pornography, introduces unnecessary procedural complexities during the trial phase.

4. The Interplay with the Information Technology Act, 2000

Given the limitations of the BNS, cyber-cells heavily rely on the IT Act to prosecute digital offenses. However, these provisions also falter when confronted with AI-generated content:

1. Section 66E (Violation of Privacy): This section criminalizes the intentional capturing, publishing, or transmitting of the image of a “private area” of any person without consent. Similar to Section 77 of the BNS, the statutory language assumes the existence of a real private area that has been captured. If the body in the deepfake belongs to an anonymous pornographic actor or is entirely AI-generated, and only the victim’s face is superimposed, it technically falls outside the strict ambit of Section 66E^[10].

2. Sections 67 and 67A (Obscenity and Sexually Explicit Content): These sections punish the publishing or transmitting of obscene material or material containing sexually explicit acts in electronic form. While prosecutors successfully use Section 67A to penalize the transmission of deepfakes, these sections focus on the “lascivious” or corrupting nature of the material to public morality, not on the specific harm of algorithmic identity theft and non-consensual fabrication^[11].

5. The Substantive Void and its Empirical Consequences

The resulting jurisprudential landscape is highly fragmented. To build a case against a deepfake creator, a prosecutor must currently patch together Section 356 BNS (for reputational harm), Section 67A of the IT Act (for electronic transmission of sexually explicit material), and potentially Section 318 BNS (cheating, if deception is involved).

This fragmented approach leads to highly vulnerable chargesheets. Empirical observation of pre-trial proceedings reveals that this substantive void directly contributes to the “Liar’s Dividend” discussed in Chapter 1. Because the law does not specifically recognize the act of synthetic fabrication as an independent sexual offense, defense strategies focus on dismantling the applicability of traditional statutes one by one, capitalizing on the lack of specific statutory definitions for AI-generated manipulation.

The Procedural Labyrinth: Decoding Section 63 BSA and the Crisis of Digital Authentication

1. The Transition to the BSA: A Paradigm of Electronic Parity

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), effective July 1, 2024, was heralded as a necessary modernization of India’s law of evidence, explicitly designed to accommodate the digital age. A central pillar of this modernization is the legal parity granted to electronic and digital records alongside traditional paper documents. The BSA replaces the convoluted jurisprudence surrounding Section 65B of the repealed Indian Evidence Act (IEA) with Section 63, which governs the admissibility of electronic records^[12].

Under Section 63 of the BSA, any information contained in an electronic record, whether printed on paper or stored in optical/magnetic media, is deemed a “document.” If the conditions of Section 63(2) are satisfied – primarily requiring a certificate affirming the functioning of the computer system and the lawful custody of the device – the electronic record becomes admissible without the need to produce the original source. However, empirical observations of trial court proceedings involving cyber-sexual offenses reveal a critical procedural labyrinth when this framework is applied to Generative AI and deepfakes.

2. The “Source vs. Content” Authentication Gap

The fundamental legislative oversight in Section 63 of the BSA is its technological presumption: it assumes that if a machine is operating correctly, the data it produces or stores is an accurate representation of reality. Section 63 certifies the integrity of the storage medium and the custody chain, not the ontological truth of the pixel-level content^[13].

In cases of deepfake sexual offenses, the computer system used to generate the synthetic media is, in fact, operating flawlessly according to its algorithmic programming. When a prosecutor submits an allegedly fabricated video extracted from an accused’s smartphone, a Section 63 certificate merely validates that the video file was indeed recovered from that specific device. It provides zero forensic value regarding whether the human faces depicted in the video were physically present or superimposed via a Generative Adversarial Network (GAN). Consequently, the BSA’s procedural safeguard creates a “Source vs. Content” gap, rendering the primary statutory mechanism for electronic admissibility entirely blind to AI manipulation.

3. The Operationalization of the “Liar’s Dividend” in Trial Courts

This authentication gap directly facilitates the legal phenomenon known as the “Liar’s Dividend.”^[14] Because Section 63 cannot inherently distinguish between a genuine recording and a hyper-realistic deepfake, the mere theoretical availability of deepfake technology heavily biases the evidentiary ecosystem in favor of the defense.

Empirical analysis of early defense strategies post-July 2024 indicates a recurring pattern in trial courts:

1. The prosecution submits digital evidence of a sexual offense (e.g., a video capturing the act), supported by a valid Section 63 certificate.
2. The defense does not contest the custody of the video but contests its authenticity, alleging it to be a deepfake engineered to frame the accused.
3. Because the trial judge lacks the technical expertise to visually discern a high-quality deepfake from genuine footage, the presumption of authenticity is shattered.

By simply raising the specter of AI manipulation, the defense successfully shifts an extraordinary burden of proof back onto the prosecution. The prosecution must now prove a negative – that the video was not altered by AI – which falls outside the scope of standard police investigation parameters^[15].

4. The Forensic Bottleneck: Overreliance on Section 39 BSA

To bridge the gap left by Section 63, trial courts are increasingly compelled to invoke Section 39 of the BSA (Opinion of Experts). Judges are routinely directing contested digital evidence to Central and State Forensic Science Laboratories (CFSLS and FSLs) to ascertain whether the media contains synthetic artifacts, mismatched frame rates, or algorithmic blending errors indicative of a deepfake^[16].

However, this reliance on Section 39 has precipitated a severe systemic bottleneck. Data collated from regional cyber-crime tribunals highlights that traditional FSLs are grossly under-resourced in terms of deep-learning forensic tools. The software required to detect GAN-generated anomalies is highly specialized and rapidly becomes obsolete as AI models (such as diffusion models) evolve.

Furthermore, the queue for forensic analysis in state laboratories often spans several months to over a year. During this protracted period, the trial is effectively paralyzed. For victims of deepfake sexual offenses – whose trauma is exacerbated by the continued, often viral, existence of the non-consensual media – this procedural delay translates to an egregious denial of timely justice.

Empirical Findings: The “Liar’s Dividend” in Practice and the Forensic Bottleneck in Trial Courts

1. Introduction to the Empirical Assessment

While doctrinal analysis highlights the statutory voids within the Bharatiya Nyaya Sanhita, 2023 (BNS) and the procedural inadequacies of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), assessing the true impact of deepfake technology requires a ground-level empirical evaluation. This chapter bridges the theoretical propositions established in previous chapters with quantitative data on cybercrime trends and qualitative assessments of trial court infrastructure, specifically focusing on forensic capacity and the practical deployment of the “Liar’s Dividend.”

2. Quantitative Trajectories: The Surge in Technology-Facilitated Sexual Violence

To contextualize the judicial burden, it is imperative to examine the epidemiological trajectory of cybercrimes in India. The latest comprehensive data from the National Crime Records Bureau (NCRB) indicates a highly alarming trend. In its most recent report detailing crime up to 2023 (published prior to the BNS enforcement but reflecting the immediate baseline), the NCRB documented 86,420 cybercrime cases, representing a staggering 63.14% surge compared to 2021^[17].

Within this matrix, offenses categorized under online sexual exploitation, blackmail, and fake profiles – the primary vectors for non-consensual deepfake pornography – accounted for over 4,000 formally registered cases. Crucially, socio-legal experts argue that this official data represents merely a fraction of the actual prevalence. Due to the deep social stigma associated with sexualized media in

India and a historically low conversion rate of National Cybercrime Reporting Portal (NCRP) complaints into formal First Information Reports (FIRs) – often hovering below 3% – the true volume of deepfake sexual offenses is vastly underrepresented in state data^[18]. As the BNS took effect in July 2024, the courts inherited this rapidly escalating, fundamentally under-reported crisis of digital violence.

3. Qualitative Observations: The “Liar’s Dividend” at the Framing of Charges

To understand how the BNS and BSA are operationalized, this study qualitatively analyzed a sample of interlocutory applications and bail hearings in regional cyber tribunals from August 2024 to early 2026. The findings unequivocally confirm the systemic exploitation of the “Liar’s Dividend.”

Under the new Schedule attached to Section 63 of the BSA, the certificate required for the admissibility of electronic evidence is bifurcated: Part A is to be filled by the party producing the record, and Part B must be executed by an “expert^[19].” When prosecutors introduce a digital file containing sexually explicit material, they frequently rely on Part A, authenticating the extraction of the file (e.g., noting the MD5 or SHA-256 hash value).

However, defense counsels are increasingly adopting a standardized counterstrategy: they do not deny the existence of the file but categorically deny the authenticity of the individuals depicted, alleging algorithmic fabrication (a deepfake). By leveraging the statutory ambiguity surrounding who qualifies to sign Part B of the Section 63 certificate, the defense effectively paralyzes the admissibility of the primary evidence. The trial courts, lacking the technical capacity to visually discern hyper-realistic synthetic media, are forced to presume manipulation until proven otherwise. This epistemological shift transfers an insurmountable burden onto the victim and the prosecution, allowing perpetrators of genuine digital sexual violence to hide behind the theoretical possibility of AI fabrication^[20].

4. The Forensic Bottleneck: Analyzing FSL Pendency

Once a trial court invokes Section 39 of the BSA (Opinion of Experts) to resolve the deepfake dispute, the digital evidence is transferred to the state’s forensic infrastructure. Our empirical investigation into the operational capacity of Indian Forensic Science Laboratories (FSLs) and Central Forensic Science Laboratories (CFSLS) reveals a systemic bottleneck that critically undermines the right to a speedy trial (Article 21 of the Constitution).

Data procured regarding the National Cyber Forensic Laboratory (NCFL) and regional cyber labs highlights a severe asymmetry between caseloads and forensic human resources. For example, recent institutional reports indicated that specialized cyber forensic divisions often operate with single-digit in-house experts supplemented by contractual staff, tasked with managing hundreds of highly complex, computationally heavy digital examinations^[21].

The forensic detection of deepfakes requires advanced computational resources and highly specialized software capable of analyzing pixel-level inconsistencies, unnatural blinking patterns, and biometric mapping errors (often requiring the deployment of reverse-GAN technology). Standard regional FSLs are predominantly equipped for

traditional mobile forensics (data extraction and basic cyber-hygiene) rather than sophisticated deep-learning analysis. Consequently, the pendency rate for analyzing contested synthetic media can extend from several months to over a year. During this forensic hiatus, the BNS/BSA trial is effectively stalled, and the victim is frequently subjected to the continued dissemination of the non-consensual media, resulting in severe secondary victimization.

Recommendations and Legal Reforms

1. The Imperative for a New Jurisprudence

The preceding doctrinal analysis and empirical findings demonstrate that the current criminal framework – comprising the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Sakshya Adhiniyam (BSA) – is conceptually and procedurally inadequate to combat the proliferation of deepfake sexual offenses. To dismantle the “Liar’s Dividend” and alleviate the forensic bottlenecks paralyzing trial courts, India requires a calibrated, multi-pronged legal reform strategy. This chapter proposes substantive amendments, evidentiary re-calibrations, and structural capacity-building measures.

2. Substantive Reforms: Enacting a Sui Generis Offense in the BNS

The reliance on fragmented provisions such as Section 77 (voyeurism) or Section 356 (defamation) of the BNS fails to capture the unique algorithmic harm of synthetic media.

1. **Recommendation:** The legislature must introduce a *sui generis* (standalone) provision within the BNS specifically criminalizing “Digital Forgery and Algorithmic Fabrication of Intimate Content.” This provision must:

2. **Decouple from Physicality:** Explicitly state that the *actus reus* does not require the physical capture of a victim, but rather the unauthorized algorithmic synthesis of their biometric data (face, voice, or body).
3. **Tiered Mens Rea:** Establish graded punishments based on intent – distinguishing between creation for personal consumption, creation for targeted harassment, and dissemination for commercial/political disruption^[22].

3. Procedural Reforms: Re-calibrating the BSA for Synthetic Media

Section 63 of the BSA currently guarantees the integrity of the storage device but is blind to pixel-level manipulation.

1. **Recommendation:** The BSA requires a specialized chapter or an amendment to Section 63 dedicated to “Digitally Manipulated and Synthetic Evidence.”
2. **Mandatory Digital Provenance:** For electronic evidence to be admissible without expert intervention, the law should gradually mandate the integration of cryptographic hashing and metadata provenance standards (such as the C2PA standard) at the hardware level (smartphones/cameras)^[23].

Reversing the Burden of Proof: To counter the “Liar’s Dividend,” the BSA should adopt a conditional reversal of the burden of proof. If the prosecution establishes the digital provenance of a file (e.g., tracing it to a specific device via ISP logs and IP addresses), the burden must shift to the

defense to provide *prima facie* technical evidence of AI manipulation, rather than allowing them to rely on mere verbal assertions to stall the trial.

Structural Reforms: Augmenting Forensic and Judicial Capacity

Legal amendments are sterile without the infrastructural capacity to enforce them. The current pendency in Central and State Forensic Science Laboratories (CFSs/FSLs) is a critical failure point.

1. **Recommendation:** AI-Specific Forensic Nodes – The Ministry of Home Affairs (MHA), in collaboration with MeitY, must establish decentralized, AI-specific forensic nodes separate from traditional cyber-forensic labs. These nodes must be equipped with continuously updated reverse-GAN detection algorithms.

2. **Judicial Sensitization:** The National Judicial Academy must implement mandatory, recurring training modules for district and sessions judges on the algorithmic mechanics of deepfakes and the proper evaluation of Section 39 BSA expert testimonies concerning synthetic media^[24].

Conclusion

The advent of Generative AI has precipitated an epistemological crisis within the Indian criminal justice system, transforming digital evidence from an objective witness into a highly contested battleground. This empirical study evaluated the efficacy of the newly implemented Bharatiya Nyaya Sanhita (BNS) and Bharatiya Sakshya Adhiniyam (BSA) in addressing deepfake sexual offenses. The doctrinal analysis reveals a highly fragmented jurisprudential landscape. Because the BNS lacks specific statutory definitions for AI-generated manipulation, prosecuting agencies are forced to patch together traditional statutes – such as outraging modesty, voyeurism, or defamation. This substantive void creates vulnerable chargesheets and allows defense strategies to dismantle the applicability of traditional statutes one by one. Procedurally, while Section 63 of the BSA streamlines the admission of routine electronic records, it relies on a binary understanding of digital evidence (tampered vs. untampered) that AI has rendered obsolete. The statute guarantees the integrity of the storage medium but is epistemologically ill-equipped to certify the ontological truth of the pixel-level content.

Empirically, these legislative and procedural gaps starkly contrast with the modernized intent of the new criminal bills. The data illustrates that while technology-facilitated sexual offenses are expanding exponentially, the legal system’s capacity to process them is constricting. The procedural mandates of Section 63 BSA, combined with the substantive voids in the BNS, have inadvertently weaponized systemic delays, placing an insurmountable burden on under-resourced forensic infrastructure.

Answers to Research Questions

1. **Research Question 1:** Trial courts empirically assess authenticity under Section 63 BSA by largely outsourcing truth-determination to MeitY-empaneled forensic laboratories. Because Section 63 leaves a critical “content gap,” courts are forced into an

overreliance on Section 39 BSA (expert opinion), which paralyzes the trial process.

2. **Research Question 2:** The primary hurdle in establishing *mens rea* and *actus reus* is the lack of a specific provision for algorithmic fabrication. Prosecutors must stretch archaic concepts to fit synthetic crimes, leading to fragile chargesheets easily challenged during framing.

Evaluation of Hypotheses

1. **Hypothesis 1 is Proved:** Procedural safeguards under Section 63 BSA are insufficient to independently authenticate hyper-realistic deepfakes. Without integrating AI-specific evidentiary presumptions, the resultant reliance on standard FSLs leads to systemic bottlenecks and prolonged trial delays.
2. **Hypothesis 2 is Proved:** The absence of a *sui generis* offense actively facilitates the “Liar’s Dividend.” This is no longer a theoretical academic concept but an empirically observable, highly successful defense strategy that thrives on the lack of judicial technical expertise to cast reasonable doubt on genuine digital evidence.

Ultimately, while the transition to the BNS and BSA was a necessary step toward decolonizing and modernizing Indian criminal law, the current statutes inadvertently provide a procedural shield for perpetrators of deepfake-facilitated sexual violence. Until the legislature bridges the substantive voids with tailored offenses and fortifies the BSA with AI-resilient evidentiary standards, deepfake technology will continue to serve as a potent, legally insulated weapon for gender-based cyber-violence.

References

1. Citations and empirical data synthesized from recent judicial observations (e.g., Delhi High Court John Doe orders regarding personality rights, 2025) and academic analyses on synthetic media.
2. The Bharatiya Nyaya Sanhita, 2023, and The Bharatiya Sakshya Adhiniyam, 2023, enforced with effect from July 1, 2024.
3. Analysis derived from the limitations of the Information Technology Act, 2000, vis-à-vis non-consensual algorithmic imagery.
4. Doctrinal review of Section 63 of the BSA, replacing Section 65B of the IEA.
5. Concept popularized in contemporary socio-legal studies regarding AI and evidentiary law, reflecting the shifting burden of proof in digital crimes.
6. Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753.
7. The Bharatiya Nyaya Sanhita, 2023, Sec. 77 (India).
8. Based on qualitative analyses of preliminary cyber-crime tribunal orders and High Court interventions quashing mismatched BNS charges in synthetic media cases during the 2024-2025 judicial cycle.
9. Supreme Court of India jurisprudence on strict construction of penal statutes; see generally, precedents establishing the requirement of physical or immediate apprehension of force for offenses akin to assault.
10. The Information Technology Act, 2000, Sec. 66E (India). This statutory gap highlights the lag between legislative drafting and rapid advancements in Generative AI.
11. Analysis of the legislative intent behind the IT Act’s obscenity provisions, which were primarily drafted to curb traditional cyber-pornography rather than targeted identity weaponization.
12. The Bharatiya Sakshya Adhiniyam, 2023, Sec. 63 (India). For legislative intent, see Parliamentary Standing Committee on Home Affairs, Report No. 248 on the Bharatiya Sakshya Bill, 2023.
13. Analysis drawn from the Supreme Court’s historical jurisprudence on electronic evidence (e.g., Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal), transposed onto the new BSA framework, highlighting the persistent limitations regarding content veracity.
14. Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147-155.
15. Qualitative assessment based on interlocutory applications filed in district and sessions courts challenging digital evidence under the nascent BSA framework (August 2024 – early 2025).
16. The Bharatiya Sakshya Adhiniyam, 2023, Sec. 39 (India). The application of expert opinion is increasingly becoming mandatory rather than discretionary in cases involving contested digital media.
17. National Crime Records Bureau (NCRB), Crime in India 2023 (Ministry of Home Affairs, Government of India). The data highlights a rapid escalation in cybercrimes, setting the immediate baseline prior to the enforcement of the new criminal laws.
18. Based on empirical assessments of the National Cybercrime Reporting Portal (NCRP), where the conversion rate of digital complaints to formal FIRs remains critically low, particularly in cases involving gendered cyber-violence.
19. The Bharatiya Sakshya Adhiniyam, 2023, Schedule to Section 63. The bifurcation into Part A (party) and Part B (expert) has introduced significant procedural friction in the authentication of digital records.
20. Qualitative analysis drawn from observing defense strategies in metropolitan cyber-crime tribunals post-July 2024, where the presumption of AI manipulation is routinely used to contest the *mens rea* and *actus reus* under BNS provisions.
21. Institutional data regarding pendency at the National Cyber Forensic Laboratory and regional FSLs, highlighting the acute shortage of trained deep-learning forensic analysts required for BSA Section 39 compliance.
22. See generally, recommendations by the Law Commission of India on the necessity of tailored digital offenses, extrapolated to the context of Generative AI.
23. The Coalition for Content Provenance and Authenticity (C2PA) provides technical specifications that, if adopted statutorily, could serve as a conclusive presumption of digital authenticity under the BSA.
24. Qualitative assessments from legal practitioners emphasize that without targeted judicial training, even the most robust forensic reports are subject to misinterpretation during cross-examination.