ARTICLE

DEEPFAKE CRIMES AND CRIMINAL JUSTICE: EVALUATING INDIA'S LEGAL RESPONSE UNDER THE BHARATIYA NYAYA SANHITA, 2023

Kimika Bhardwaj* & Dr. Shruti Goyal**

Abstract

The criminalisation of synthetic media in India has not been a planned phenomenon; it is the result of a nineteenth-century categorisation of media that was designed to address nineteenth-century harms. This article makes a doctrinal analysis of the current legal response to deepfake crimes under the Bharatiya Nyaya Sanhita, 2023 ("BNS"), read together with the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. It argues that the BNS was drafted in the very period in which generative AI was mainstreamed in India, yet was formulated without any awareness of this new category of synthetic media, and hence merely re-numbers rather than resolves the interpretive tension that the Indian Penal Code, 1860 had already shown when confronted with morphed images and voice cloning. The article examines the constitutional underpinnings in Articles 19 and 21, the developing personality and publicity-rights jurisprudence of the Delhi High Court, and a comparative study of the European Union's Artificial Intelligence Act and the United States' TAKE IT DOWN Act, to show how India's personation, forgery, defamation and voyeurism provisions together create a disjointed, victim-unfriendly, and largely civil rather than criminal enforcement pathway.

Keywords Deepfakes; Bharatiya Nyaya Sanhita, 2023; Synthetic Media; Personality Rights; Digital Criminal Justice.

I. INTRODUCTION

A fake video that cast the actor Rashmika Mandanna as a character dressed in a British-Indian style and entering an elevator went viral in India on social media in November 2023, before it was revealed that her face had been synthesised onto the body of another influencer[1].

This incident was not the first or the worst example of synthetic impersonation seen in India, but it played an important role in a rhetorical process, taking a technical curiosity that had been discussed primarily in cyber-security forums to the level of a public and parliamentary issue. The Union Government issued advisory letters to intermediaries within days, and within three years the architecture of intermediary regulation in India was significantly restructured to accommodate what the law now officially refers to as "synthetically generated information".[2]

* LL.M. in Criminal Law, Rajiv Gandhi National University of Law, Patiala
** Associate Professor of Law, Rajiv Gandhi National University of Law, Patiala

[1] See generally Press Release, Ministry of Electronics & Information Technology, *Advisory to Intermediaries on Deepfakes and AI-Generated Content* (Dec. 26, 2023).

[2] Ministry of Electronics & Information Technology, *Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026* (Feb. 10, 2026).

The focus of this article is a narrower, but arguably more fundamental question: can the substantive criminal law of India, namely the Bharatiya Nyaya Sanhita, 2023, [3] effectively prosecute the harms caused by deepfakes? It is important to note that the timing of the BNS's drafting coincides with the mainstreaming of generative artificial intelligence. The Bharatiya Nyaya Sanhita Bill was introduced in the Lok Sabha just as the flood of synthetic media and algorithmically generated content began reaching Indian consumers, yet nowhere in the Sanhita is there any direct or indirect mention of synthetic media, AI or algorithmic content. [4] What emerged instead was a re-numbered and somewhat modernised version of the colonial penal code, which -- in response to the falsification of paper documents and the physical impersonation of one person by another -- had included offences such as cheating by personation, forgery, criminal defamation and voyeurism. These offences face three challenges when applied to deepfakes: first, the near-complete resemblance of fabricated content to authentic content, which collapses the real/fake distinction that the law of forgery always assumed; second, the absence of any direct relationship between perpetrator and victim, which is a problem for offences premised on a deceptive impression created upon a specific person, as in cheating; and third, the scale and reach of digital transmission, which renders remedies designed for individual wrongs -- such as an injunction, a defamation suit, or a complaint under Section 66C of the Information Technology Act, 2000 -- structurally inadequate to the harm.

The article proceeds in eight parts. This introduction is followed by a historical overview of the law of forgery and impersonation, from the colonial codes to the BNS. Part III situates the discussion within the constitutional guarantees of privacy, dignity and equality, and the Supreme Court's evolving interpretation of them. Part IV maps the existing legal landscape across the BNS, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the IT Rules, 2026. Part V examines the emerging judicial response, which has so far been sought largely through civil suits on personality rights before the Delhi High Court rather than through criminal prosecution. Part VI undertakes a comparative study of the European Union and the United States. Part VII sets out, in pointwise form, the critical doctrinal issues and the contemporary institutional challenges facing enforcement. Part VIII presents the article's conclusions together with proposed reforms. [5]

II. HISTORICAL EVOLUTION

Encountering impersonation and fabrication through criminal law is not a new phenomenon in India; it dates back long before the digital age. The Indian Penal Code, 1860, drafted under Lord Macaulay, contained a forgery provision and a cheating-by-personation provision, both premised on the paradigmatic case of a physical document -- a will or a promissory note -- being forged, or of a person physically impersonating another in a transaction or in writing a letter to another.[6] For more than a century the Code's assumptions of authorship, authenticity and personal interaction held up well, because fabrication technology was relatively unsophisticated -- handwriting, seals, and

[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India) (notified Feb. 10, 2026).
[4] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023) (effective July 1, 2024).
[5] See infra Parts II–VIII.
[6] K.D. GAUR, *Textbook on the Indian Penal Code* (7th ed. 2023).

manipulation in the photographic darkroom -- and the requirement to prove a specific false representation made to a specific deceived person did not buckle under scale. [7]

The passage of the Information Technology Act, 2000 brought the first major disruption. The Act was amended in 2008, on the recommendation of an expert committee, to add Section 66C on identity theft, Section 66D on cheating by personation through a computer resource, and Section 66E on violation of bodily privacy. These provisions were reactive rather than anticipatory: they responded to a rising tide of email fraud, fake social-media identities and spying. The three-year punishment they prescribe reflects the rough measure of harm from identity fraud in the early Web 2.0 era, not the harm caused by a hyper-realistic, non-consensual synthetic video within moments of upload.

The second major development was the Bharatiya Nyaya Sanhita, 2023. The Standing Committee on Home Affairs, which reviewed the three new criminal codes, extensively examined cyber crime, organised crime and terrorism, yet its report contains no substantive discussion of synthetic media, deepfakes, or the liability of those who fabricate a person's likeness using generative tools. Sections 75-78 make only incidental modernising gestures, such as expressly including an "electronic record" within the concept of a document for forgery purposes. The Sanhita was written, debated and passed between 2022 and 2023 -- precisely the period in which consumer-grade face-swap and voice-cloning tools were released to the public, letting anyone manipulate faces and voices within minutes. This omission was not born of technological obscurity, as the drafters of 1860 might plausibly have claimed; it is instead a structural feature of the codification exercise itself. [8] The Sanhita was conceived as a decolonising and consolidating project -- renaming, renumbering and pruning colonial-era offences such as sedition and unnatural offences -- rather than as an occasion for new, forward-looking criminalisation. The result is that India's criminal-justice response to deepfakes has remained confined largely to interpretive stretching of the Sanhita, while the real regulatory activity has occurred through executive rule-making under the Information Technology Act and through civil litigation before the High Courts.

III. CONSTITUTIONAL FRAMEWORK

The constitutional issues relevant to deepfake criminalisation run along three dimensions: [9] the right to privacy and dignity under Article 21; freedom of speech and expression under Article 19(1)(a), read with the reasonable restrictions in Article 19(2); and the guarantee of equality under Articles 14 and 15, which acquires special significance here because deepfake harms fall disproportionately on women. The starting point is the nine-judge bench decision in Justice K.S. Puttaswamy v Union of India, which held that the right to privacy is part of the right to life and personal liberty under Article 21 and includes the right to informational self-determination -- an individual's right to control information about herself. At its core, a deepfake is an invasion of informational self-determination: it creates and circulates a representation of the data subject's body, voice or likeness engaged in conduct the subject never performed and never consented to. The doctrinal difficulty is that

[7] RATANLAL & DHIRAJLAL, *The Indian Penal Code* (35th ed. 2022).
[8] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code §§ 2(9), 336 (2023).
[9] See generally Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Puttaswamy was decided against the backdrop of state surveillance and the Aadhaar architecture, so its extension to a purely private deepfake -- created by one private individual against another, with no state action involved -- remains constitutionally undeveloped. The earlier decision in R Rajagopal v State of Tamil Nadu, which recognised a common-law right to privacy in one's name, likeness and life story against unauthorised commercial exploitation, is therefore the more direct doctrinal anchor, and it is Rajagopal -- not Puttaswamy -- that underlies the Delhi High Court's personality-rights jurisprudence discussed in Part V. [10]

The second axis is freedom of speech. Deepfake technology is not inherently unlawful and is used extensively for satire, parody, film dubbing, accessibility tools and artistic commentary, all protected under Article 19(1)(a). Any criminal prohibition addressing deepfake harm must therefore be carefully calibrated so that it does not capture protected expression or fall foul of the vagueness and chilling-effect objections that were raised against Section 66A of the Information Technology Act, 2000 in Shreya Singhal v Union of India. A purpose-based distinction -- between deceptive, harm-causing synthetic content on one hand, and disclosed, satirical or consensual synthetic content on the other -- offers a constitutionally sounder route to defining "harm" than a blanket prohibition on the underlying technology, which is the approach now attempted through the labelling architecture of the IT Rules, 2026.

The third and most pressing axis, in the Indian context, is equality. Non-consensual deepfake pornography is overwhelmingly directed at women, as documented in journalistic and civil-society accounts, making it a form of gendered harm that falls within Article 15(1)'s prohibition on sex discrimination and within the special-provision power in Article 15(3). The BNS's voyeurism, sexual-harassment and outraging-modesty provisions (Sections 75, 77 and 79), drafted in the wake of the Justice Verma Committee recommendations following the 2012 Delhi gang-rape case, could not have anticipated synthetic imagery. The case for a constitutional, harm-based gendered offence is therefore strong: Article 15(3) could ground a substantive response in an area where the formal remedies of cheating, forgery and defamation have plainly failed to stem the volume of gendered synthetic abuse now being documented under the IT Rules, 2026.

IV. EXISTING LEGAL POSITION

Bharatiya Nyaya Sanhita, 2023

India has never had dedicated legislation on deepfakes or synthetic media; the existing framework is an amalgamation of four statutes -- the BNS, 2023, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended in 2026) -- none of which took synthetic media as its organising concern[11]. Depending on how a deepfake is used, at least six provisions of the BNS could be invoked. Cheating by personation under Section 319 is engaged when synthetic video or audio is used to induce a victim to part with property, as in digital-arrest or family-emergency frauds where a cloned voice mimicking a relative or law-enforcement officer demands a wire transfer. Section

[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), as amended by Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India).

[11] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code §§ 75, 77, 319, 336, 351, 356 (2023).

336 on forgery, which extends the Sanhita's definition of "document" to electronic records, applies where a synthetic video is tendered as a genuine record -- for instance, in matrimonial or employment disputes. Section 356 on criminal defamation applies where a deepfake damages a victim's reputation, regardless of whether the content was AI-generated. Section 351 on criminal intimidation applies where a deepfake is used or threatened to coerce a victim, most commonly in sextortion cases built on synthetic explicit imagery. Sections 75, 77 and 79, covering sexual harassment, voyeurism and outraging modesty, may also be engaged in some fact patterns.

The Information Technology Act, 2000

The BNS operates alongside the Information Technology Act, 2000, whose Sections 66C, 66D and 66E remain in force; police routinely register first information reports under both statutes for the same conduct. While the Sanhita's narrower voyeurism provision covers only sexual acts and applies only to women, Sections 67 and 67A of the IT Act -- which criminalise the electronic dissemination of obscene and sexually explicit material respectively -- are the principal pathway for the gravest category of harm, non-consensual synthetic intimate imagery. [12]

The Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 does not mention deepfakes and carries no criminal offence provisions; it is enforced through civil monetary penalties imposed by the Data Protection Board. Its definition of "personal data", however, is broad enough to cover the facial geometry, voiceprint and other biometric markers that a deepfake model extracts to generate or modify content, and its consent regime under Sections 4 and 6 generally requires a lawful basis before a person's biometric likeness can be used to train or fine-tune a generative model. The Act's utility is nonetheless limited, since it does not expressly address web-scraped training data and offers no criminal remedy. [13]

The IT Rules, 2021 (as amended in 2026)

Significant intermediaries must, where technically feasible, ensure a prominent visual and audible indication that content has been generated, added, omitted or modified using computer resources, and must embed a unique identifier or permanent metadata that traces the content back to the resource used to create or alter it. Intermediaries must also act on government instructions concerning unlawful synthetic material within three hours -- the fastest statutory takedown deadline anywhere in the world -- on pain of losing the safe-harbour protection under Section 79 of the IT Act. These Rules represent a genuine regulatory innovation, but they are directed solely at intermediaries and create no new criminal liability for the person who creates or first uploads a deepfake; liability for that primary wrongdoer continues to rest on the BNS provisions described above. [14]

---

[12] Information Technology Act, No. 21 of 2000, India Code §§ 66C, 66D, 66E (2000); Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).
[13] Digital Personal Data Protection Act, No. 22 of 2023, India Code § 33 (2023).
[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), r. 3 (India).

V. JUDICIAL INTERPRETATION

The most striking feature of the Indian judicial response to deepfakes is its almost exclusive location in civil litigation rather than criminal prosecution -- specifically, commercial suits filed before the Delhi High Court seeking injunctions grounded in personality and publicity rights. This pattern matters doctrinally: it suggests that the BNS's criminal provisions have not yet produced a meaningful body of trial-court decisions addressing AI-generated content, while civil courts have moved comparatively quickly and liberally to recognise a right against synthetic misappropriation of identity. The doctrinal foundation for this civil relief traces back to Rajagopal's recognition of a privacy interest in one's own likeness, and to Titan Industries Ltd v Ramkumar Jewellers, which first articulated an Indian common-law right of publicity protecting the commercial value of a celebrity's identity against unauthorised appropriation.

In Anil Kapoor v Simply Life India, the actor sought to restrain the unauthorised commercial exploitation of his name, voice, image and other personality attributes -- including through AI-generated deepfakes and unconnected product endorsements. The issue before the Delhi High Court was whether an ex-parte, ad-interim injunction could extend beyond the named defendants to unnamed future infringers. Justice Prathiba Singh's order is notable for its explicit engagement with the underlying technology, observing that AI tools now let any unauthorised user recreate a person's persona, and for extending the injunction to "the world at large" -- a formulation broad enough to bind domain registrars and even the Department of Telecommunications and the Ministry of Electronics and Information Technology, both impleaded to assist enforcement. [15]

In Amitabh Bachchan v Rajat Nagi, the actor had first secured protection against the unauthorised use of his name, image and voice in a fake lottery scheme; a subsequent Delhi High Court order extended that protection specifically to future unauthorised use of AI-generated images and audio built from his voice and face. The issue here was less about the initial fraud than about future-proofing the injunction against a harm -- synthetic impersonation -- that had not existed in its present form when the original suit was filed.

In Jackie Shroff v The Peppy Store, the Delhi High Court restrained the commercial use of the actor's likeness and identity by AI systems and chatbots built from his facial features. The issue in this case was whether personality-rights protection extends to AI systems and conversational bots trained on a person's image, and not merely to static or video content -- a question the Court answered in the affirmative, further widening the civil doctrine.

Together, these decisions establish an emerging civil doctrine under which a person's name, voice, image, signature style and other unique personality attributes are treated as protectable property, defensible through injunctions that are frequently ex parte and broadly framed against unnamed future infringers. No comparable body of criminal case law has yet developed under Sections 319, 336, 356 or 77 of the BNS in relation to deepfakes, though police in several States have registered first information reports invoking these sections, mostly in voice-cloning fraud cases. This absence should be read not as an indication that no such cases exist, but as a sign that the interpretive questions identified in Part IV -- whether the "capturing of images" language in Section 77 extends to deepfake creation, or whether Section 336's forgery framework, built around falsifying an existing

[15] *R. Rajagopal v. State of Tamil Nadu*, MANU/SC/0056/1995.

document, can stretch to cover a wholly fabricated one -- have not yet been tested on appeal. Until a higher court rules, the law's application to deepfakes remains unsettled.

A related line of cases concerns the constitutionality of executive regulation of synthetic and misleading content generally. In Kunal Kamra v Union of India[16], the Bombay High Court held that the amended Rule 3(1)(b)(v) of the IT Rules, 2021 -- which empowered a government-appointed Fact Check Unit to flag "fake, false or misleading" information about government business -- was unconstitutionally vague and violated Articles 14 and 19(1)(a). The Court's reasoning on Article 19(2) has significant implications for the labelling and takedown architecture of the 2026 Amendment Rules, and any future constitutional challenge to those Rules will likely be tested against Kunal Kamra's requirement of narrow, precisely defined criteria.

VI. COMPARATIVE ANALYSIS

Comparing the European Union and the United States reveals two distinct regulatory philosophies against which the Indian position can be measured: the EU's transparency-first, provider-and-deployer model, and the United States' harm-specific, victim-remedy model.

6.1 Explanation of the European Union's Strong Law

The EU's Artificial Intelligence Act, Regulation (EU) 2024/1689, is widely regarded as the most developed transparency regime for synthetic media anywhere in the world. Its key features are:

- Article 50 imposes transparency obligations that apply regardless of whether the underlying AI system is classified as high-risk.
- Providers of systems that generate synthetic audio, image, video or text carry a technical obligation to mark that output in a machine-readable format.
- Deployers who use such systems to produce content resembling a real, identifiable person carry a separate obligation to disclose that the content was artificially generated or manipulated. [17]
- The level of required disclosure is context-sensitive, and is relaxed where the content is evidently artistic, satirical or fictional.
- The Act separates the roles of provider and deployer, attaching distinct obligations to each rather than regulating the technology as a single undifferentiated activity.
- It is fundamentally a labelling and provenance regime, not a criminal offence regime -- creating a harmful deepfake is not itself made a crime under the Act.
- It does not supply a standalone definition of "deepfake" or a corresponding legal test, leaving that task to member states. [18]

[16] *Kunal Kamra v. Union of India*, 2024:BHC-OS:14750-DB, Writ Petition (L) No. 9792 of 2023 (Bom. H.C. Sept. 20, 2024) (India).

[17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689), art. 50.

[18] Information Technology Act, No. 21 of 2000, India Code § 79 (2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, rr. 3, 7 (India).

6.2 The United States

The American response is the most narrowly targeted at the most serious category of harm, while also being the most fractured. In the absence of federal legislation, a mosaic of state laws governs different aspects of synthetic media -- including Tennessee's ELVIS Act of 2024, which bars AI-generated simulations of a person's voice without consent -- alongside the federal TAKE IT DOWN Act, which came into force in May 2025. The TAKE IT DOWN Act is instructive precisely because of its narrowness: rather than regulating synthetic media generally, it targets the single highest-harm use case, non-consensual intimate imagery, whether authentic or AI-generated, and pairs individual criminal liability with a time-limited notice-and-removal process administered by the Federal Trade Commission rather than the criminal courts. This bifurcated design -- individual criminal liability alongside platform-facing civil regulation -- is structurally cleaner than the Indian position, where the BNS addresses the individual perpetrator (albeit inadequately) and the IT Rules, 2026 address the platform, with no statutory cross-reference linking the two regimes. [19]

VII. CRITICAL ISSUES AND CONTEMPORARY CHALLENGES

The analysis above points to seven doctrinal and institutional problems, set out here in pointwise form.

1. Absence of a deepfake-specific mens rea and actus reus. Every BNS provision currently relied upon in deepfake cases was drafted around a different fact pattern and requires judicial stretching to accommodate synthetic generation. The stretching is not costless: the private creation and storage of a non-consensual synthetic intimate image, without publication, is unlikely to satisfy either Section 336 (intent to use a forged document as genuine) or Section 77 (capturing or publishing an image of a real event).

2. Misaligned classification of offences. Section 319 (cheating by personation) is non-cognizable, meaning police cannot investigate without a magistrate's order; Section 356 (defamation) is bailable and compoundable at the magistrate's discretion. These classifications are not matched to the speed of digital harm, since most reputational and psychological damage from a deepfake occurs within the first few hours of circulation, well before a victim can secure a magistrate's order. [20]

3. A two-tier remedy structure. The most developed remedy -- the omnibus personality-rights injunction, as in Anil Kapoor -- is realistically available only to plaintiffs who can fund a commercial suit against a sophisticated infringing network. Ordinary victims of deepfake fraud or non-consensual intimate imagery, who make up the vast majority of those affected, are left with the blunter and slower route of a criminal complaint under the BNS or the IT Act.

4. An evidentiary vacuum. The Bharatiya Sakshya Adhiniyam, 2023 creates no presumption, burden-shifting rule or special procedure for authenticating digital evidence alleged to be AI-generated. Section 63, which governs the admissibility of electronic records, retains the old requirement of proving the authenticity of an electronic record's origin, without addressing whether the recording itself is authentic. In the absence of a forensic-authentication protocol comparable to

[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India).
[20] Regulation (EU) 2024/1689, *supra* note 17, art. 50(2), (4).

the Coalition for Content Provenance and Authenticity framework, trial courts must determine authenticity ad hoc through expert testimony, with no statutory presumption to rely on.

5. Limited investigative capacity. AI-content detection increasingly requires tools and training that most State and district cybercrime cells lack. The National Cyber Crime Reporting Portal centralises complaint intake, but there is no consistent link between the number of complaints received and the number of cases actually investigated.

6. Jurisdictional and extraterritorial gaps. The platforms on which deepfakes circulate, and often the servers that generate them, are based outside India. The IT Rules, 2026 apply to significant intermediaries regardless of location once a threshold number of Indian users is crossed, but how the three-hour takedown obligation is to be enforced against offshore infrastructure remains unaddressed.

7. Electoral vulnerability. India's linguistic diversity and multi-platform political communication make it especially vulnerable to synthetic media during election periods, including AI-generated recordings of political leaders -- in at least one instance, of a deceased leader -- used in campaigning. The Election Commission's Model Code of Conduct contains no specific provision on synthetic media, and while Section 353 of the Code of Criminal Procedure, 1973 (incitement to public mischief) and Section 319 of the Representation of the People Act, 1951[21] (corrupt practices) could in theory be stretched to cover deepfake-driven electoral manipulation, neither was drafted with this scenario in mind, and the compressed timeline of an election leaves little room for the sustained investigation Section 319 ordinarily requires. [22]

VIII. CONCLUSIONS AND SUGGESTIONS

Reforms

The analysis above supports four reform proposals, each designed to preserve the doctrinal structure the BNS has already built while closing its gaps.

First, an offence of non-consensual synthetic personation. Parliament should enact a clear prohibition -- either as a new BNS provision on offences against the human body and reputation, or as a corresponding amendment to Section 66 of the IT Act, 2000 -- against creating or disseminating a synthetic audio, image or video representation of a clearly identifiable person that a reasonable viewer would believe to be genuine, with aggravated punishment where the content is sexually explicit, used to solicit property, or targets a minor. Consistent with the Article 19(2) analysis in Part III, the offence should turn on the absence of consent and the potential for deception, not on the mere use of AI technology, so that disclosed satire, parody and consensual content remain outside its scope.

Second, reclassification of aggravated categories as cognizable and non-bailable. Where a synthetic-personation offence involves sexually explicit material, a minor, or financial fraud, it should be classified so as to permit police investigation without prior magisterial authorisation.

[21] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code §§ 77, 319, 336, 356 (2023).
[22] Ensuring Likeness, Voice, and Image Security Act, Tenn. Code Ann. § 47-25-1101 et seq. (2024); TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55 (2025).

Third, a provenance-based evidentiary presumption. The Bharatiya Sakshya Adhiniyam, 2023 should be amended to create a rebuttable presumption that content lacking the provenance metadata or labelling required under the IT Rules, 2026, but bearing characteristics that a court-recognised forensic protocol associates with AI generation, is synthetic. This would assist both prosecutors and civil litigants without requiring the prosecution to prove synthetic origin from first principles in every case.

Fourth, statutory integration between the BNS and the IT Rules, 2026. The current silo -- platform obligations to label or act under delegated IT Act legislation, and individual criminal liability under the BNS, with no link between them -- should be replaced by an explicit provision treating a platform's failure to label or act, in violation of the IT Rules, as admissible evidence of constructive notice, aligning the incentives of the two regimes rather than leaving them to operate in parallel.

The Bharatiya Nyaya Sanhita, 2023 was drafted against a backdrop of technological change it does not recognise. Its provisions on cheating by personation, forgery, defamation, criminal intimidation and voyeurism can be -- and are being -- stretched to cover deepfake conduct, but at the cost of uncertain coverage, a procedural classification scheme misaligned with the speed of digital harm, and an evidentiary framework silent on how to establish the authenticity of synthetic content. The Delhi High Court's emerging personality-rights jurisprudence is moving faster than the criminal law, but an injunction of the kind granted in Anil Kapoor and Amitabh Bachchan v Rajat Nagi is no substitute for criminal deterrence, nor is it realistically available to the ordinary citizen who is most likely to be victimised by deepfake-driven fraud or non-consensual intimate imagery. The IT Rules, 2026 provide a useful intermediate labelling and takedown regime, but one directed at platforms rather than at the wrongdoer whom the criminal law exists to deter and punish. A comparative look at the European Union's transparency-first approach and the United States' harm-based TAKE IT DOWN Act suggests that India's continued reliance on general-purpose, nineteenth-century penal categories is neither the only nor the most defensible legislative option. The reforms proposed above a new offence of synthetic personation, reclassification of offence cognizability, an evidentiary presumption keyed to content provenance, and a statutory link between the BNS and the IT Rules -- are doctrinally modest, but together they would help close the accountability gap that currently lets the creators of the most harmful synthetic content exploit the space between a criminal code that does not name their conduct and a regulatory regime that does not punish it.