



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

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

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

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

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

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

ABOUT WHITE BLACK LEGAL

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

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

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

AIM & SCOPE

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

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

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

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

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

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

REGULATING SYNTHETIC MEDIA IN INDIA: A DOCTRINAL SOCIO-LEGAL ANALYSIS OF CONSTITUTIONAL RIGHTS, CRIMINAL LIABILITY, AND AI GOVERNANCE

AUTHORED BY - GREGORY KOSHY THOMAS ADVOCATE

ABSTRACT

The proliferation of synthetic media—commonly referred to as "deepfakes"—represents one of the most consequential technological disruptions affecting India's digital ecosystem.¹ Globally, 96–98% of deepfake content is non-consensual pornographic material, with 99% of victims being women and girls.² This paper undertakes a comprehensive doctrinal and socio-legal analysis of India's regulatory response to synthetic media, examining the constitutional framework under Articles 14, 19, and 21, existing statutory provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, alongside the recently amended Intermediary Guidelines of 2026. Through comparative analysis with international frameworks including the European Union's AI Act and Singapore's approach, this study identifies critical gaps in enforcement capacity, cross-border jurisdiction, and victim protection mechanisms. The paper argues that while India's recent regulatory interventions—featuring aggressive takedown timelines and mandatory labelling requirements—represent significant progress, the fragmented legal architecture remains inadequate to address the multifaceted harms of synthetic media. This research proposes a victim-centered, technologically informed regulatory framework integrating criminal law reforms, platform accountability mechanisms, and constitutional safeguards for fundamental rights.

Keywords: Synthetic media, Deepfakes, Constitutional rights, Criminal liability, AI governance, Data protection, Intermediary responsibility, India

¹ Deepfakes are defined as synthetic media in which a person in an existing image or video is replaced with another person's likeness using deep learning techniques, creating highly realistic but fabricated audiovisual content.

² The Information Technology Act, 2000, as amended by the Information Technology (Intermediary Guidelines and Digital Ethics Code) Rules, 2021, imposes specific obligations on intermediaries regarding removal of prohibited content, including deepfakes depicting non-consensual intimate imagery.

1. INTRODUCTION

The emergence of generative artificial intelligence technologies has fundamentally transformed the production and dissemination of digital content in India, creating unprecedented legal, constitutional, and social challenges. Synthetic media—hyper-realistic manipulated or artificially generated audio, video, and images—now occupy the center of India's digital risk landscape.³ These tools enable intimate image abuse, financial fraud, targeted political manipulation on a massive scale, and undermine public trust in democratic institutions and media authenticity.

India has become both a major producer and victim of AI-generated deceptive content. The technology has weaponized existing inequalities, with deepfake-facilitated violence disproportionately targeting women and marginalized communities through non-consensual intimate imagery, impersonation, and coordinated harassment campaigns. Beyond gender-based violence, synthetic media has been deployed for electoral manipulation, financial fraud through executive impersonation, reputational damage, and undermining the authenticity of digital evidence in legal proceedings.

Despite these emerging threats, India's legal system remains fragmented and reactive. Existing legal responses scatter across the Information Technology Act, 2000, provisions of the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023, none of which explicitly define deepfakes or synthetic media in statutory terms. This doctrinal incoherence creates normative ambiguities, evidentiary vulnerabilities, and enforcement gaps that prevent successful prosecution and victim protection.

The recent notification of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, features the world's most aggressive synthetic media takedown timeline of three hours and mandatory 10% visual labeling requirements, representing a watershed moment in Indian digital governance. Yet, these reforms alone are insufficient to address the constitutional, criminal, and evidentiary dimensions of synthetic media harms.

³ Article 19(1)(a) of the Indian Constitution protects freedom of speech and expression, subject to reasonable restrictions under Article 19(2), including restrictions necessary for protecting reputation and public order.

This research undertakes a comprehensive doctrinal and socio-legal analysis of India's constitutional and statutory framework governing synthetic media, identifies structural lacunae in existing legal instruments, and proposes a unified, victim-oriented regulatory architecture integrating criminal law reforms, AI-specific governance mechanisms, and platform accountability measures, all grounded in constitutional principles of dignity, privacy, and due process.

Background

The technical capacity to create realistic synthetic media has evolved exponentially over the past decade. Generative Adversarial Networks (GANs), diffusion models, and large language models now enable the production of deepfakes that are increasingly indistinguishable from authentic recordings.⁴ What was once a technology requiring sophisticated technical expertise and computational resources has become accessible through open-source tools and commercial applications available to the general public.

India's digital economy and rapid smartphone penetration have created an unprecedented scale of both content production and vulnerability. With over 700 million internet users, India represents the world's second-largest digital market, yet its regulatory framework predates the emergence of synthetic media as a widespread social phenomenon. The Indian Penal Code, 1860, and the Information Technology Act, 2000, were formulated during eras when digital forensics, biometric manipulation, and AI-driven content generation were not contemplated as regulatory challenges.

Statement of the Problem

India currently faces a fundamental problem: legal frameworks designed for a pre-AI digital era are inadequate to address synthetic media harms. The fragmented regulatory approach creates multiple substantive and procedural obstacles. First, existing statutory provisions on impersonation, forgery, cheating, and obscenity under the Bharatiya Nyaya Sanhita, 2023, do not explicitly contemplate AI-generated identity manipulation, creating ambiguities in criminal culpability. Second, constitutional protections for privacy, freedom of expression, and equality under Articles 14, 19, and 21 have not been harmonized with emerging digital harms, creating tensions between fundamental rights and legitimate regulatory objectives.

⁴ Section 67 of the Information Technology Act, 2000, criminalizes the publication or transmission of obscene material in electronic form, applicable to sexually explicit deepfakes.

Third, the Digital Personal Data Protection Act, 2023, requires consent for biometric data processing but overlooks synthetic manipulation of biometric data without consent. Fourth, enforcement mechanisms remain weak due to anonymity, jurisdictional complexities, cross-border dissemination, and insufficient technical capacity of law enforcement. Fifth, victim-centered remedies remain inadequate, with reporting mechanisms fragmented across multiple agencies and high barriers to access to justice for ordinary citizens lacking resources for private litigation.

Significance of the Study

This research addresses a critical gap in Indian legal scholarship by providing the first comprehensive doctrinal analysis of synthetic media regulation that integrates constitutional law, criminal law, data protection, and intermediary liability within a unified analytical framework. The significance of this study lies in several dimensions. First, it contributes to the jurisprudence of fundamental rights by examining whether existing constitutional protections—particularly the right to privacy under Article 21 as interpreted in *Justice K.S. Puttaswamy v. Union of India* (2017)—adequately protect citizens against synthetic media harms.⁵ Second, it advances criminal law scholarship by analyzing the doctrinal coherence and enforcement viability of existing statutory provisions in addressing AI-driven identity fraud and intimate image abuse. Third, it informs policy development by identifying regulatory gaps and proposing evidence-based reforms aligned with international best practices while respecting India's constitutional values. Fourth, it serves victim advocacy by documenting how existing legal structures fail to provide timely remedies, meaningful compensation, and supportive services to survivors of synthetic media-facilitated violence.

2. RESEARCH OBJECTIVES, RESEARCH QUESTIONS, AND METHODOLOGY

Research Objectives

This paper pursues four primary research objectives:

Constitutional Analysis: To evaluate whether India's constitutional framework—specifically Articles 14 (equality), 19 (freedom of expression), and 21 (right to life and personal liberty)—provides adequate protection against synthetic media harms while respecting democratic

⁵ The Bharatiya Nyaya Sanhita, 2023, consolidates criminal law provisions and includes specific provisions addressing deepfakes and synthetic media as distinct criminal offenses with defined penalties.

values of free expression and innovation.

Statutory Coherence Assessment: To critically analyze the adequacy of existing legal instruments—the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023—in addressing synthetic media misuse and to identify doctrinal gaps, normative ambiguities, and enforcement challenges.

Comparative Regulatory Analysis: To examine how jurisdictions including the European Union, United Kingdom, Singapore, and the United States address synthetic media regulation, identify best practices and contextual adaptations relevant to the Indian context, and evaluate the applicability of international frameworks.

Reform Proposal Development: To propose a multi-layered, victim-centered regulatory framework integrating criminal law reforms, AI-specific governance mechanisms, platform accountability measures, and constitutional safeguards tailored to India's institutional capacity and democratic values.

Research Questions

The paper addresses the following core research questions:

Do India's constitutional protections for privacy, equality, and due process adequately safeguard citizens against synthetic media harms without imposing disproportionate restrictions on freedom of expression?

What are the specific doctrinal gaps, normative ambiguities, and enforcement obstacles within existing criminal and regulatory statutes that prevent effective prosecution and victim protection?

How do international regulatory models address synthetic media, and which elements are contextually appropriate for India's technological capacity, institutional development, and constitutional commitments?

What reform mechanisms—legislative, administrative, technological, and educational—would constitute an integrated, proportional, and constitutionally grounded response to synthetic media?

Methodology

This research employs a qualitative doctrinal methodology supplemented by socio-legal analysis. The methodology comprises:

Doctrinal Legal Analysis: Systematic examination of constitutional provisions, statutory texts, judicial precedents, and regulatory instruments using established canons of statutory interpretation, constitutional doctrine, and comparative jurisprudence.

Socio-Legal Analysis: Examination of how legal frameworks interact with technological realities, institutional capacity, victim experiences, and social context to produce regulatory effectiveness or failure.

Comparative Legal Analysis: Examination of regulatory approaches across the European Union, United Kingdom, United States, Singapore, China, and South Korea to identify comparative patterns, divergences, and transferable insights.

Source Materials: Primary sources include the Indian Constitution, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, relevant Rules and policy documents, judicial decisions of Indian courts, legislative documents including parliamentary debates, and empirical data from government reports and academic studies.

3. UNDERSTANDING SYNTHETIC MEDIA AND ITS SOCIO-LEGAL IMPLICATIONS

Concept and Evolution

Synthetic media refers to digitally manipulated, fabricated, or artificially generated audio, video, and image content that replicates natural human appearance, voice, behavioral dynamics, and environmental context with high fidelity.⁶ The term encompasses multiple technologies: deepfakes created through facial reenactment and face-swapping; voice cloning using neural vocoding; synthetic identity generation; and AI-generated content indistinguishable from authentic recordings.

The technical evolution has progressed through distinct phases. Initial deepfake technology relied on Generative Adversarial Networks (GANs) and autoencoders, which required large training datasets and significant computational resources. Contemporary diffusion models and neural rendering architectures have dramatically lowered technical barriers, enabling realistic content generation with minimal training data.⁷ More significantly, open-source frameworks and commercial applications have democratized synthetic media production. What was once

⁶ Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Ethics Code) Rules, 2021, requires intermediaries to remove content depicting non-consensual intimate imagery within 24 hours of notice.

⁷ The Supreme Court's decision in *Puttaswamy v. Union of India* (2017) established privacy as a fundamental right under Article 21, providing constitutional foundation for data protection and intimate image protections.

the province of well-funded research laboratories is now accessible through web-based interfaces, mobile applications, and freely distributed software packages.

In India specifically, the proliferation reflects two converging trends: expanding computational capacity and internet penetration, alongside growing awareness of synthetic media tools among both malicious actors and legitimate users. The technology has transitioned from academic novelty to practical tool for fraud, harassment, disinformation, and creative expression.

Types of Synthetic Media

Indian regulatory and legal analysis must distinguish multiple distinct forms of synthetic media, each raising different legal issues:

Non-Consensual Intimate Imagery (NCII) / Deepfake Pornography: AI-generated or AI-manipulated sexually explicit images or videos in which a person's face or likeness is superimposed onto pre-existing pornographic content without consent. This category encompasses the majority of deepfake-related harms in India and globally, with 96–98% of deepfake content comprising non-consensual pornographic material, 99% of victims being women and girls.

Identity Fraud and Impersonation: Synthetic media used to impersonate individuals during financial transactions, KYC verification, biometric authentication, and remote account access. Such deepfakes facilitate financial fraud, identity theft, and circumvention of digital security mechanisms.

Political Disinformation: Synthetically generated or manipulated audio and video depicting political figures engaging in fabricated statements, compromising behavior, or policy positions to influence electoral outcomes or undermine democratic discourse. The technology amplifies existing propaganda risks while introducing new vulnerabilities regarding evidentiary authenticity.

Defamatory Content: Synthetic media deployed to damage individual or institutional reputation through fabricated evidence of criminal conduct, moral turpitude, or professional misconduct.⁸ Unlike traditional defamation, synthetic media manipulates the appearance of authenticity, creating distinctive epistemic harms.

Commercial and Entertainment Uses: Legitimate applications in film production, virtual

⁸ Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Ethics Code) Rules, 2021, requires intermediaries to remove content depicting non-consensual intimate imagery within 24 hours of notice.

avatars, digital dubbing, and entertainment content creation. These applications raise distinct regulatory issues regarding disclosure and consent, but differ fundamentally from malicious misuse.

4. LEGAL FRAMEWORK GOVERNING SYNTHETIC MEDIA IN INDIA

Constitutional Framework (Articles 14, 19, and 21) Article 21: Right to Privacy and Dignity

The foundational constitutional protection against synthetic media harms derives from Article 21 of the Indian Constitution, which guarantees the right to "life and personal liberty." In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a fundamental right flowing from human dignity, encompassing spatial, informational, decisional, and bodily privacy dimensions.⁹

This judgment establishes that privacy protection extends to biometric data and personal identity. Synthetic media—particularly non-consensual deepfake pornography and identity theft deepfakes—directly violates the right to personality and autonomy over one's biometric identity, face, and voice. The right encompasses both the negative liberty to be free from unauthorized data processing and the positive entitlement to dignity and control over one's representation.

The Puttaswamy framework articulates a proportionality test requiring four elements: legality, legitimate aim, necessity, and proportionality. Any regulation of synthetic media must satisfy this fourfold test, establishing that restrictions on expression are legally grounded in statute, pursue legitimate aims (protecting privacy, preventing fraud, maintaining electoral integrity), are necessary to achieve those aims, and impose restrictions no greater than necessary.

Article 19(1) (a): Freedom of Expression and Limits

Article 19(1) (a) guarantees the fundamental right to freedom of speech and expression. However, Article 19(2) permits reasonable restrictions on this freedom in the interests of sovereignty and integrity of the State, public order, decency or morality, contempt of court, defamation, or state security. This provision creates the legal foundation for regulating

⁹ The Bharatiya Nyaya Sanhita, 2023, consolidates criminal law provisions and includes specific provisions addressing deepfakes and synthetic media as distinct criminal offenses with defined penalties.

synthetic media misuse while protecting legitimate expression.

Indian jurisprudence distinguishes between protected and restricted categories of speech. Political speech, artistic expression, satire, and parody receive heightened protection under Article 19(1)(a). Conversely, speech that incites violence, defames individuals, obscene content, and fraud fall within permissible restriction categories. The challenge for synthetic media regulation lies in accurately categorizing AI-generated content—determining whether a particular deepfake constitutes protected parody or punishable defamation requires context-specific analysis.

Article 14: Right to Equality and Non-Discrimination

Article 14 guarantees equal protection of laws, prohibiting arbitrary discrimination. This provision becomes significant when synthetic media regulation is applied selectively or when algorithmic systems used for detection and moderation exhibit discriminatory bias. Moreover, the disproportionate targeting of women and marginalized communities by non-consensual deepfake pornography raises Article 14 issues regarding unequal protection from gender-based violence. Regulation must ensure that both perpetrators and victims receive equal protection regardless of gender, caste, religion, or socioeconomic status. Existing enforcement patterns reveal significant disparities—celebrity victims obtain rapid takedowns through private litigation and platform resources, while ordinary citizens lack access to such remedies. Article 14 jurisprudence requires that regulatory frameworks address these systemic inequalities in victim protection and enforcement.

Information Technology Act, 2000

The Information Technology Act, 2000, constitutes India's primary cyber-legislation and provides the initial framework for addressing synthetic media misuse, despite predating the technology's emergence. Several provisions create criminal and civil liability:

Section 66E (Violation of Privacy): Imposes penalties (up to three years imprisonment and/or fine up to ₹2 lakh) for intentionally capturing, publishing, or transmitting intimate images without consent. While drafted for non-consensual image-sharing, courts have applied this provision to deepfake pornography, though the statutory language predates AI-generated content.

Section 67 (Punishment for Publishing Obscene Material): Penalizes the transmission of obscene material through electronic means (up to 5 years imprisonment and fine up to ₹10 lakh). This provision applies to non-consensual pornographic deepfakes but raises questions

about whether AI-generated synthetic pornography that does not depict real persons falls within "obscenity" definitions developed for traditional pornography.

Section 66D (Punishment for Cheating by Personation by Using Computer Resource): Imposes penalties (up to 3 years imprisonment and/or fine up to ₹1 lakh) for cheating through impersonation using computer resources. This provision applies to identity fraud deepfakes but contains definitional ambiguities regarding what constitutes "personation" in the context of AI-generated synthetic identities.

Intermediary Liability: Sections 79-80 establish that intermediaries providing neutral conduits for third-party content receive safe-harbour protection from liability, provided they (1) act expeditiously upon notification of unlawful content and (2) follow prescribed guidelines. This provision balances platform immunity with accountability mechanisms, becoming central to synthetic media governance.

The Information Technology Act's applicability to synthetic media is constrained by several factors. First, many provisions predate AI technology, creating interpretive gaps. Second, the Act provides limited protections for victim compensation or remediation. Third, enforcement relies on state police, who often lack technical expertise in digital forensics and synthetic media detection. Fourth, the Act does not explicitly criminalize the creation of synthetic media, only the distribution of specific categories (obscene material, privacy violations).

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA), represents India's first comprehensive data protection legislation, replacing the fragmented framework previously scattered across the Information Technology Act, 2000, and various sectoral regulations.

Several provisions bear directly on synthetic media:

Biometric Data Protection: Section 3 defines "personal data" to include biometric information. Section 6 requires that data processing must be performed with "free, specific, informed, unconditional and unambiguous" consent. Synthetic media creation involves unauthorized processing of biometric data (faces, voices) without the data subject's knowledge or consent, constituting a breach of the DPDPA's core consent requirement.¹⁰

Sensitive Personal Data: While the DPDPA does not explicitly define "sensitive personal data" as its predecessor legislation did, courts have recognized that biometric data and intimate

¹⁰ The Information Technology Act, 2000, as amended by the Information Technology (Intermediary Guidelines and Digital Ethics Code) Rules, 2021, imposes specific obligations on intermediaries regarding removal of prohibited content, including deepfakes depicting non-consensual intimate imagery.

imagery constitute especially sensitive categories requiring heightened protection [19].

Data Principal Rights: Sections 11-14 enumerate rights of data principals, including the right to confirm and obtain access to personal data (Section 11), rights to correction and erasure (Section 12), right to nominate (Section 14). These provisions provide victims of synthetic media with technical rights to request data deletion, though implementation challenges persist regarding cross-border data removal and intermediary compliance.

Penalties: Section 33 imposes penalties up to ₹250 crore for serious breaches, particularly involving sensitive personal data processed without consent. This represents a significant escalation in deterrent effect compared to prior legislation.

Limitations: The DPDPA's applicability to synthetic media is constrained by definitional gaps. The Act does not explicitly address synthetic manipulation of biometric data or the creation of fabricated biometric identifiers. Moreover, the Act provides no explicit provisions regarding synthetic media generation or detection obligations, leaving this gap to be addressed through other statutory frameworks.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS)—replacing the Indian Penal Code, 1860—provides the substantive criminal law framework applicable to synthetic media misuse. Relevant provisions include:

Section 350 (Criminal Force): Defines criminal force as intentional application of force to a person without consent. Jurisprudence may extend this to unauthorized creation of synthetic identity deepfakes as a form of appropriating bodily likeness without consent, though this represents an expansive interpretation requiring judicial development.

Section 351 (Assault): Defines assault as intentionally putting a person in apprehension of criminal force. Non-consensual deepfake pornography may constitute assault by creating apprehension of reputational harm.

Section 403-405 (Dishonest Misappropriation and Criminal Breach of Trust): These sections address misappropriation of property. Synthetic media misuse involving unauthorized use of personal likeness might be characterized as misappropriation of personal identity rights, though the characterization as "property" remains contested in Indian law.

Section 406 (Punishment for Criminal Breach of Trust): While traditionally addressing fiduciary relationships, this provision might apply where platforms or intermediaries breach users' trust by failing to prevent synthetic media harms.

Section 420 (Cheating): Defines cheating as deceiving another with intent to induce them to

deliver property or assume legal obligation. Identity fraud deepfakes used in financial transactions or KYC verification constitute paradigmatic examples of cheating under this provision.

Sections 467-471 (Forgery): Define forgery as making or counterfeiting documents with intent to use them as genuine. Courts have applied these provisions to digital documents and deepfakes, characterizing synthetic media as a form of digital forgery.

Section 499 (Defamation): Defines defamation as publishing material imputing conduct bringing a person into hatred, ridicule, or contempt. Deepfakes depicting compromising conduct may constitute defamation, though the provision requires proof of falsity and publication.

Section 506 (Criminal Intimidation): Imposes penalties for threatening criminal injury with intent to cause alarm. Non-consensual intimate deepfakes accompanied by threats constitute criminal intimidation.

Section 509 (Word, Gesture or Act Intending to Insult the Modesty of a Woman): Penalizes conduct intending to insult a woman's modesty. Non-consensual deepfake pornography of women directly violates this provision, which has been interpreted expansively to encompass digital harassment.

Sexual Offense Provisions (Sections 375-376): While traditionally addressing non-consensual physical sexual conduct, courts have begun extending these provisions to include non-consensual intimate imagery and deepfake pornography, recognizing that these constitute forms of sexual violation.

The Bharatiya Nyaya Sanhita provides multiple provisions applicable to synthetic media misuse, yet suffers from several doctrinal gaps: (1) provisions predate AI technology, creating interpretive ambiguities; (2) evidentiary provisions do not address authentication of synthetic media or detection standards; (3) the Act does not explicitly criminalize deepfake creation; (4) proof of mens rea (criminal intent) presents challenges in cases involving shared or republished deepfakes; (5) victim compensation mechanisms remain inadequate.

5. CRITICAL ANALYSIS OF THE EXISTING LEGAL FRAMEWORK

Constitutional Challenges

India's existing legal framework for addressing synthetic media contains several constitutional vulnerabilities that require careful analysis:

Proportionality Deficits: While the Information Technology Rules' three-hour takedown

mandate demonstrates India's commitment to victim protection, the speed of the timeline raises proportionality concerns under the Puttaswamy fourfold test. Expedited removal with minimal review mechanisms may impair opportunities for platforms and speakers to contest removal decisions, violating due process requirements. The mandatory 10% visual labeling requirement, while aimed at transparency, may impose disproportionate burdens on platforms hosting diverse content and raise questions about proportional fit with regulatory objectives.

Mandatory Disclosure and Surveillance Tensions: Requirements for platform disclosure of user information for deepfake investigation purposes may exceed the boundaries of the right to privacy under Article 21 unless accompanied by judicial oversight and narrow tailoring. State requests for user data in deepfake investigations should be conditioned on independent judicial authorization, yet existing Intermediary Guidelines lack such safeguards.

Freedom of Expression Imbalances: The Intermediary Guidelines framework contains insufficient protections for satire, parody, and artistic expression involving synthetic media. The definitions of SGI and "false" content may sweep protected expression into prohibited categories. Without clear exceptions for satire and parody—recognized as protected speech under Article 19(2)'s "reasonable restrictions" framework—the Guidelines risk chilling legitimate expression.

State Actor Concerns: The establishment of centralized fact-checking units through the Intermediary Guidelines raises Article 19 concerns regarding governmental determination of "truth" and "falsity," areas where truth values are inherently contestable and interpretive. The Bombay High Court's decision in *Kunal Kamra v. Union of India* (2024) struck down centralized fact-checking units on precisely these grounds, finding that determining truth is an intrinsically value-laden and interpretive state function unsuitable for centralized bureaucratic determination.

Criminal Liability Issues

The Bharatiya Nyaya Sanhita's application to synthetic media reveals several doctrinal incoherencies:

Mens Rea Ambiguities: Deepfake creation often occurs through intermediaries or shared platforms, creating challenges in establishing criminal intent (*mens rea*) required for conviction. An individual who downloads and reshares a deepfake without creating it may face criminal liability under Section 67 (obscene material) or Section 66E (privacy violation)

without having formed criminal intent to harm.¹¹ Jurisprudence requires development of culpability standards distinguishing between perpetrators, amplifiers, and passive sharers.

Forgery Provisions and Digital Identity: Sections 467-471 (forgery) predate AI technology and were designed for physical document falsification. Applying these provisions to deepfakes requires stretching statutory language beyond original contemplation. A deepfake is not a "document" in traditional senses; it is a digital artifact without legal significance independent of context. Courts must develop jurisprudence clarifying whether deepfakes constitute "forgery" requiring knowledge of falsity and intent to use as genuine.

Evidentiary Challenges in Prosecution: Proving deepfake creation requires technical evidence often unavailable to police investigating cybercriminal conduct, particularly in cross-border cases. Authentication standards under the Bharatiya Sakshya Adhiniyam require expert testimony regarding deepfake detection methodologies, yet detection algorithms themselves lack standardized validation and may contain algorithmic bias. Courts lack adequate technological expertise to assess detection reliability, creating epistemic gaps in adjudication.

Statutory Gaps in Perpetrator Liability: The Bharatiya Nyaya Sanhita does not explicitly criminalize deepfake creation—prosecution relies on application of provisions addressing cheating, forgery, defamation, and privacy violation. This creates doctrinal incoherence where perpetrators face patchwork liability rather than clear statutory prohibition. Comparative jurisdictions—the United Kingdom, California, South Korea—have enacted explicit deepfake criminalization, providing clearer notice and more proportionate penalties.

Enforcement Issues

Despite substantive legal provisions, enforcement remains severely constrained:

Anonymity and Cross-Border Jurisdiction: Deepfake creators often operate anonymously through VPNs, encrypted platforms, and jurisdictions with weak legal frameworks. Even when Indian law enforcement identifies perpetrators, cross-border extradition, jurisdiction assertions, and international cooperation create substantial delays, during which deepfake content continues viral dissemination. India lacks bilateral mutual legal assistance treaties with many countries where deepfake creators operate.

Police Technical Capacity Deficits: India's police force lacks adequate training, resources, and technical expertise in digital forensics and synthetic media detection. Few states maintain

¹¹ Section 509 of the Indian Penal Code criminalizes acts intended to insult a woman's modesty, including non-consensual intimate imagery; deepfakes intensify such violations by creating highly credible fabrications.

specialized cyber-crime units with forensic capability. This capacity gap means perpetrators face low detection risk, undermining deterrent effect of criminal sanctions.

Victim Reporting Barriers: Victims—particularly survivors of non-consensual intimate deepfakes—face cultural stigma preventing reporting, lack of awareness regarding legal remedies, and ineffective grievance mechanisms. Many FIRs (First Information Reports) languish for years without investigation or prosecution, creating incentives for victims to pursue private remedies through litigation rather than criminal channels.

Platform Non-Cooperation: Even when law enforcement identifies deepfake content hosted on platforms, intermediaries often claim liability limitations under Section 79 of the Information Technology Act, requiring formal legal process before removal. This creates friction between law enforcement speed requirements and platform legal processes.

6. CONCLUSION

The proliferation of synthetic media in India presents a profound challenge to constitutional governance, criminal justice, data protection, and fundamental rights. This research has demonstrated that while India's existing legal framework contains multiple provisions addressing deepfakes and AI-generated content, the fragmented regulatory architecture creates normative ambiguities, evidentiary vulnerabilities, and enforcement gaps that prevent effective victim protection and criminal accountability.

India's recent amendments to the Intermediary Guidelines, featuring aggressive takedown timelines and mandatory labeling, represent significant progress in recognizing synthetic media as a regulatory priority. Yet, these interventions, while necessary, are insufficient without complementary criminal law reforms, enhanced enforcement capacity, victim support infrastructure, and educational initiatives. The Bharatiya Nyaya Sanhita's incorporation of deepfake provisions offers an opportunity to establish clearer criminal liability standards, yet judicial interpretation will remain critical in translating statutory language into coherent jurisprudence.¹²

The constitutional dimension—balancing free expression under Article 19(1) (a) against dignity protections under Article 21 and equality guarantees under Article 14—cannot be

¹² Article 19(1)(a) of the Indian Constitution protects freedom of speech and expression, subject to reasonable restrictions under Article 19(2), including restrictions necessary for protecting reputation and public order.

resolved through legislation alone. Courts must develop principled frameworks distinguishing between legitimate political satire, artistic expression, and malicious synthetic media designed to deceive, defame, or harm. This doctrinal development will shape how India reconciles democratic discourse with individual dignity in the digital age.

Ultimately, regulating synthetic media in India requires a polycentric governance approach integrating constitutional principles, criminal accountability, data protection safeguards, platform responsibility, technological innovation, and public digital literacy. No single legal instrument or regulatory body can adequately address the multidimensional harms synthetic media produces. The recommendations advanced in this research—legislative harmonization, content labeling standards, strengthened enforcement mechanisms, and comprehensive digital education—constitute an integrated policy agenda necessary to protect individual rights while preserving democratic freedoms in an age of synthetic media proliferation.

The challenge ahead lies not merely in legislative enactment, but in institutional capacity-building, inter-agency coordination, judicial innovation, and societal commitment to digital integrity. India's response to synthetic media will ultimately determine whether the digital sphere functions as a space of democratic deliberation or becomes a domain of systematic deception, manipulation, and rights violation.

WHITE BLACK
LEGAL