LEGAL AMENITY LAW JOURNAL – ISSN 3107-9148

Volume I Issue II November – December 2025

Synthetic Media and Legal Accountability: Why India Requires a Bespoke Deepfake Regulation Statute

By-Md Imtiaz Laskar

3rd Year Law Student, Techno India University, Kolkata, West Bengal.

ABSTRACT

Advances in artificial intelligence (AI), particularly in the form of generative models that enable the creation of synthetic audio, video, and image content ("deepfakes"), pose urgent challenges for democratic societies, individual rights, reputations, and institutional trust. This paper examines how deepfake AI is emerging as a systemic problem in internet society, how existing legal regimes in India are structurally inadequate or ill-equipped to address the scale and sophistication of harms, and why a bespoke regulatory framework is required. It highlights illustrative misuse incidents (both globally and in India), analyses current Indian constitutional and statutory provisions (with reference to the new reforms under the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA)), identifies gaps, and proposes a roadmap for reform. Comparative lessons, such as regulatory proposals abroad (e.g. Denmark's emerging statute protecting image/voice/likeness), are used to underscore the possibility and need for tailored legislation.

INTRODUCTION

In recent years, the development and proliferation of AI-generated synthetic media, commonly referred to as "deepfakes", has escalated dramatically. Deepfakes are audiovisual content (video, audio, images) produced or manipulated through machine learning and generative adversarial networks (GANs), resulting in synthetic media that appear deceptively authentic. Their realism is increasing rapidly, and the tools to generate deepfakes are becoming widely accessible for a broad population. Therefore, deepfakes pose significant risks to individual reputation and privacy, electoral integrity, public trust, creative industries (especially artists), law enforcement, national security, and more.

In the Indian context, though there is growing awareness, the legislative and regulatory framework continues to lag behind the speed and sophistication of the technology. While some existing provisions can potentially address specific harms (such as defamation, impersonation, and data protection), there is no dedicated statutory provision that comprehensively regulates

the creation, dissemination, detection, liability, and remedies for AI-generated deepfake content. This lacuna enables misuse and harms to proliferate. This paper argues for the urgent need for a new legal provision (or framework) specifically addressing deepfakes and synthetic AI-generated content, anchored within Indian constitutional protections and the recently reformed criminal statutes.

DEEPFAKE AI : DEFINITION, MECHANISM, AND SOCIETAL THREATS

What are Deepfakes?

Deepfakes refer to synthetic media produced or manipulated using artificial intelligence (AI), especially generative models such as GANs (Generative Adversarial Networks), diffusion models, or neural rendering to replace a subject's face or voice, or to generate entirely fabricated video/audio/images that convincingly imitate a real person. These manipulations range from face-swapping to voice cloning to fully synthetic persona creation.

Technological advances have led to high fidelity in generating realistic videos, audio speech, and images that are increasingly difficult to distinguish from genuine content. Detection tools have also evolved, but adversarial methods, the generation of higher resolution content, and distribution pipelines allow deepfakes to proliferate rapidly and widely. (Deepfakes in digital media forensics: Generation, AI-based detection and challenges, 2025)

Societal Risks and Harms

Deepfakes generate a wide array of harms:

1. **Misrepresentation and Impersonation**: Fake videos or audio impersonating a public figure or private individual can defame, damage reputation, or manipulate political or social discourse.
2. **Misinformation / Disinformation / Election interference**: Synthetic political videos or fake statements can mislead electorates, influence public opinion, polarise societies, or manipulate democratic processes.
3. **Fraud and Scams**: Deepfake voice cloning or video impersonation can be used for fraud scam calls, social engineering, impersonation, financial scams, etc.
4. **Harassment, Non-consensual content, Privacy Violations**: Deepfake porn, non-consensual sexual content, forged intimate videos, or synthetic media can deeply harm individuals (especially women, public persons, and vulnerable persons).

5. **Artistic and cultural harm / Copyright and misuse**: The technology can misuse or appropriate artists' styles, replicate artists' likeness or performance without consent, infringe on creative rights, lead to plagiarism, or erode trust in authenticity.
6. **Erosion of trust and public order**: When synthetic media becomes pervasive, trust in legitimate video/audio evidence can degrade, social cohesion can be damaged, and misinformation becomes more difficult to police.

These risks require systemic legal and regulatory responses.

ILLUSTRATIVE INCIDENTS AND MISUSE CASES

To highlight the gravity of the problem, consider recent real-world incidents of deepfake misuse and AI-generated content abuse: -

1. High-profile political / identity defamation deepfake cases

- Recently, a video involving the political leader Bhagwant Mann was circulated as an AI-generated (deepfake) video making inflammatory statements, which triggered a police FIR and intervention by law enforcement. Unknown persons created and shared a highly realistic video purporting to show the leader making communal statements, raising a serious threat to public order and defamation[1].
- A leading artist / public figure, Akshay Kumar, recently obtained an urgent order from the Bombay High Court for the removal of deepfake content that infringed on his personality rights. The court recognized that the deepfake video was virtually indistinguishable from reality, posed a grave danger to public order and to the person's family and reputation, and directed the removal of the material[2].

2. Widespread fear, chilling effect, especially among vulnerable groups

- There has been documented emergence of a "chilling effect" in which women in India are increasingly refraining from posting personal images or engaging publicly because of fear that their photos will be captured and misused by deepfake or "nudify" tools, leading to harassment, non-consensual image manipulation, or sexual abuse. The recent

[1] *CM Mann's AI deepfake video sparks FIR, cops tracing creator", The Times of India (Chandigarh, 21 October 2025) https://timesofindia.indiatimes.com/city/chandigarh/cm-manns-ai-deepfake-video-sparks-fir-cops-tracing-creator/articleshow/124725491.cms accessed 29 November 2025*

[2] *Truly alarming': Bombay HC orders removal of deepfake content infringing Akshay Kumar's personality rights, Times of India (Mumbai, 17 October 2025) https://timesofindia.indiatimes.com/city/mumbai/truly-alarming-bombay-high-court-orders-removal-of-deepfake-content-infringing-akshay-kumars-personality-rights/articleshow/124611724.cms accessed 29 November 2025.*

findings show that many women are withdrawing from online platforms due to concerns about deepfake misuse, and the existing legal process is slow or fragmented[3].

3. **Global regulatory developments and prospective law (Denmark example)**
   - The government of Denmark is now preparing to amend its copyright and related law to guarantee that every person has the right to their own body, facial features and voice, giving citizens explicit legal protection and the right to demand removal of deepfake content featuring them without consent. This would become among the first laws globally that treat a person's unique likeness and voice as a form of protected copyright or personality right[4].
   - Scholarly advocacy emphasises that such regulatory models restore accountability and create removal/compensation rights for victims of deepfakes.[5]
4. **Incidents of AI-voice scams / impersonation fraud**
   - There have been reported cases in India where individuals fall victim to AI-voice call scams or synthetic voice impersonations for financial fraud. For example, a lawyer in the northeastern region (Meghalaya) reportedly lost a large sum after being tricked by an AI voice call impersonation. Such scams are facilitated by the availability of deepfake/voice-cloning tools that ordinary persons can access. (As per your referenced incidents.)
   - Broader reporting suggests that deepfake fraud attempts increased manifold recently, with a sharp increase in scam attempts using synthetic video or audio targeting citizens.
   - These examples illustrate how deepfake misuse is already a grave problem in both public-figure defamation and private citizen contexts.

THE INDIAN LEGAL LANDSCAPE: CURRENT REGIME AND GAPS

Constitutional and Rights Framework

India's constitutional framework provides a range of fundamental rights which are relevant to deepfake harms.

---

[3] *India's women fear new wave of abuse as AI deepfakes spread online', **The Guardian** (5 November 2025) https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse accessed 29 November 2025.*

[4] *Denmark to tackle deepfakes by giving people copyright to their own features', The Guardian (27 June 2025) https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence accessed 29 November 2025.*

[5] *We Need Laws to Stop AI-Generated Deepfakes," **Scientific American** (The Editors, 18 November 2025) https://www.scientificamerican.com/article/we-need-laws-to-stop-ai-generated-deepfakes/ accessed 29 November 2025.*

1. **Right to Freedom of Speech and Expression (Article 19)**

   The Constitution guarantees freedom of speech and expression (Article 19) to citizens. Synthetic media content, artistic or political expression, commentary or parody potentially enjoys protection. However, this right is not absolute: reasonable restrictions may be imposed in the interests of public order, defamation, reputation, morality, or preventing incitement.

2. **Right to Life and Personal Liberty (Article 21)**

   Article 21 protects the dignity, life, and personal liberty of individuals. Personality rights, privacy, reputation, bodily integrity, identity and personal autonomy fall under the ambit of Article 21 jurisprudence. Forged videos or deepfakes that target a person's identity, dignity or misrepresent them may implicate Article 21.

3. **Personality rights, image and likeness protection**

   While Indian jurisprudence has recognised aspects of "personality rights" or "right to one's image/likeness/voice/reputation", there is no uniform codified law dedicated solely to deepfake remediation. High Courts have entertained and granted relief in specific suits involving the misuse of an individual's image or likeness, but the scope remains piecemeal, case-based, and lacks a comprehensive statutory foundation.

   Thus, the constitutional framework provides foundational protections (speech, dignity, personality rights), but given the scale, speed, and sophistication of AI-generated deepfakes, these foundational rights must be complemented with specific legal provisions tailored to deepfakes and synthetic media.

EXISTING STATUTORY AND REGULATORY PROVISION (AND LIMITATIONS)

At present, in India, a range of statutory provisions and regulatory instruments theoretically apply to deepfake creation, dissemination or harms. However, none directly address all aspects of deepfakes comprehensively.

Here is an overview of the relevant statutory landscape, with an assessment of strengths and limitations.

Statutory Framework: Key Provisions

1. **Information Technology Law (formerly under Information Technology Act, 2000 and related rules)**

- The IT Act (and associated rules and intermediary liability frameworks) provide certain protections against cybercrime, misuse of information, dissemination of harmful or obscene content, and removal obligations for intermediaries. There are also provisions around intermediaries' duties to remove certain kinds of harmful or misleading content, and regulations in the digital space. The government has recently issued statements acknowledging the threats posed by synthetic media/deepfakes and emphasized platform accountability and content removal mechanisms.
- However, the existing legislation is largely generic. It addresses cyber-offences, defamation, fake identity, obscenity, etc., but does not have a bespoke regime or statutory offence or classification for "deepfake / synthetic AI-generated content" as such. Enforcement remains reactive rather than proactively geared to synthetic media detection, watermarking, liability for creation, etc.

2. **Criminal Law Reform: Bharatiya Nyaya Sanhita (BNS) and related new legislation**
   - As per recent reforms, the Bharatiya Nyaya Sanhita (BNS) is the replacement statute for certain criminal provisions. Some commentary suggests that existing provisions will be used to address offences such as impersonation, defamation, forgery, identity fraud, and other cybercrimes. Indeed, there is academic literature pointing out that while general offences exist, there is no dedicated offence specifically for AI-driven deepfake generation, manipulation, and distribution that targets synthetic media creation or manipulative deepfake misuse in a comprehensive manner.
3. **Evidence law / procedural reforms: Bharatiya Sakshya Adhiniyam (BSA)**
   - The Bharatiya Sakshya Adhiniyam (BSA), which reforms evidentiary law and admissibility, is relevant because deepfake content (video, audio) often becomes evidence in courts. The statute must provide standards for authentication, verification, digital forensics, and criteria for admitting synthetic media or contested audiovisual evidence. However, while the reforms strengthen evidentiary frameworks, there is a limited explicit statutory provision dealing exclusively with deepfake detection standards, mandatory watermarking, technical traceability or "synthetic content authenticity obligations"
4. **Data protection / privacy / related frameworks**
   - Emerging frameworks for data protection, privacy, and digital personal data also provide protection when personal data or an individual's privacy/consent is misused. Yet again, there is no dedicated statutory provision that targets the generation of deepfake content by non-consensual means, voice cloning, or AI-generated impersonation specifically.

5. **Judicial precedents and personality-right jurisprudence**

- Some High Courts have recently intervened in deepfake cases. For example, the Bombay High Court granted urgent removal orders for deepfake content involving a public figure's likeness and ordered the takedown of AI-generated defamatory videos[6]. Similarly, other FIRs have been filed in cases involving the creation or sharing of defamatory deepfake videos involving public figures or political leaders. However, the judicial response remains ad hoc and incremental, lacking statutory clarity or specialized procedural mechanisms tailored for deepfakes.

CHALLENGES: WHY DEEPFAKES BYPASS OR STRAIN EXISTING LAWS

Even though India has a constitutional framework, a reformed criminal code, and general cyber-laws, deepfake misuse reveals multiple structural challenges. These limitations inhibit effective deterrence, detection, enforcement, and reparations.

1. **Speed and Scale vs. Reactive Legal Mechanisms:** - Deepfake generation is low-cost, widely accessible, and scales rapidly. A synthetic video or audio impersonation can be generated and disseminated across social media, messaging, and viral platforms globally within hours. Traditional law enforcement and litigation are slow processes. By the time complaints reach courts or police, the deepfake may have propagated widely, taken root in public discourse, and caused reputational or political harm. The existing system is predominantly reactive (complaint → takedown → legal proceedings), which struggles to keep pace with volume and virality.
2. **Difficulty of Detection, Attribution, and Authentication**: - Deepfake content quality is rapidly improving; high-fidelity deepfakes are increasingly difficult to distinguish. Detection tools are developing, but AI generation techniques evolve concurrently. Tracing originators (creators), establishing the server, distributed uploaders, anonymised or offshore creators, and cross-border platforms complicate attribution. In evidentiary settings, courts require authentication, forensic verification, chain of custody. Without statutory standards for watermarking, metadata preservation, mandatory watermarking of synthetic media, or platform traceability obligations, authentication is cumbersome.
3. **Gaps in Specific Offence Definitions and Legal Certainty** :- While defamation, impersonation, identity fraud, criminal intimidation, etc., are covered under general

[6] *Akshay Hari Om Bhatia v John Doe and Others, Interim Application (L) No 33184 of 2025 in Commercial IP Suit (L) No 32986 of 2025 (Bombay HC, 15 October 2025).*

criminal or civil law, there is no express statutory offence of "creation and dissemination of malicious deepfake synthetic video/audio/impersonation" that accounts for the unique nature of AI-generated content (e.g. non-consensual face/voice cloning, manipulated video or audio presented as "real" political speech). Consequently, ambiguity persists about which provision applies, the burden of proof, the threshold for intent, and remedies for victims beyond takedown.

4. **Platform Liability and Intermediary Regulation is Fragmented**: - Large social media platforms and intermediaries host synthetic content. While intermediary liability laws and takedown processes exist, there is a limited mandated standard for prioritising synthetic content, transparency for labelling, mandated visible watermarking or "deepfake detected/verified" tags, or tools for real-time detection. This regulatory gap allows harmful deepfake videos or audio to remain live for extended periods before removal or mitigation**.**
5. **Protection of Artists, Creative Expression, and Attribution: -** Deepfakes also impact artistry and creators. Artists' content, voice, style, performance, and identity can be cloned or misrepresented. For example, misuse of an artist's images, voice, or artworks through AI, or copying an artist's style/community without consent, leads to economic and moral rights harms. There is limited legal clarity on protecting artists against synthetic replication or unauthorised style cloning under existing statutes.

   Moreover, detecting and providing remedies for artists is complex: attribution, proof of derivative work, livelihood disruption, reputational damage, etc.
6. **Public Awareness, Digital Literacy, and Societal Trust: -** Many citizens may not realise a video is fake, may be misled by realistic deepfakes, share virally, and contribute to misinformation. The public's capacity to verify or challenge content is limited. Until regulatory frameworks mandate labelling, watermarking, traceability, and detection transparency, misinformation will spread unchecked.

COMPARATIVE LEGAL DEVELOPMENT AND INTERNATIONAL BEST PRACTICES

To design effective regulation, it is instructive to consider emerging international approaches. One especially relevant development is in Denmark.

Denmark's Proposed Legal Amendment on Image/Voice Likeness

The government of Denmark has introduced a bill/amendment under which every individual will have the right to their own body, facial features, and voice as a form of legal protection.

The proposal creates a statutory right over one's image, voice and facial features, thereby giving citizens standing to demand removal of deepfake content featuring them without consent. The proposed legislation is among the first globally to treat a person's unique likeness and voice as protected under a dedicated statutory regime rather than relying solely on existing tort, defamation or personality rights[7].

Commentators have described this as a potentially pioneering "copyright-style" protection over bodily likeness and voice, which would give removal remedies and compensation rights, and place clear obligations on platforms/creators.

Comparative Regulatory Trends

1. Several jurisdictions globally (e.g. European Union, United States, etc.) are debating or enacting laws/regulations requiring transparency, watermarking of synthetic media, platform obligations, consumer labelling, detection obligations, and election-period safeguards
2. Proposals emphasise mandatory visibility labels ("this video/audio contains AI-generated content"), metadata traceability, platform accountability, and dedicated offences for deepfake political manipulation, non-consensual intimate content, and identity fraud.
3. Academic and policy research suggests a rights-based approach:

- legislation combining prohibition of malicious deepfake creation/dissemination without consent,
- mandatory registration/labelling/watermarking,
- mandatory retention of provenance/metadata,
- civil and criminal redress for victims,
- mandatory transparency and platform reporting.

[7] *'Denmark to tackle deepfakes by giving people copyright to their own features', The Guardian (27 June 2025) https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence accessed 29 November 2025.*

CRITICAL ANALYSIS: WHY THE CURRENT INDIAN FRAMEWORK IS INSUFFICIENT

Despite the growing awareness and some regulatory developments in India, the current regime remains insufficient for the following reasons:

1. **Lack of a Dedicated Offence for Synthetic/Deepfake Generation**
   While general offences under the new criminal statute (BNS) or older statutes can address impersonation, defamation, forgery, or identity theft, there is no express offence that uniquely captures malicious synthetic media generation powered by AI (deepfake generation, manipulation, distribution) particularly when used for public deception or large-scale misinformation. This leads to uncertainty, inconsistent enforcement, and underdeterrence.
2. **Absence of Mandatory Labelling or Watermarking/Traceability Requirements**
   There is currently no statutory requirement that creators or platforms must embed visible, persistent digital watermarking, or metadata provenance markers in synthetic content, or label that content is AI-generated. Without a statutory traceability or labelling obligation, detection remains difficult, and harmful deepfakes persist.
3. **Procedural and Evidentiary Barriers**

   The evidentiary law (under BSA) and existing procedural mechanisms require robust forensic authentication, chain of custody, origin tracing, etc. Given the ease of cross-border, anonymous generation and distribution, and the sophistication of deepfakes, current forensic and procedural tools struggle to keep pace. There is a need for mandated standards for digital forensics, real-time detection, shifting the burden of proof in certain cases, mandatory preservation, etc.
4. **Insufficient Protection for Artists, the Creative Sector, and Personality Rights**

   Artists, creators, performers whose voice, likeness, style or artwork are replicated or misused by synthetic AI currently rely on existing remedies (personality suits, copyright, image rights, defamation), which are slow, expensive, and not specifically tailored to synthetic replication or generative AI. A statutory framework is necessary to protect artists' identity, moral rights, and economic interests in the age of synthetic replication.
5. **Fragmented Platform Accountability and Transparency**

Platforms host vast quantities of user-generated media. While there are intermediary regulations, there is no clear regime for proactive detection, labelling, transparent reporting of detected deepfakes, mandatory removal timelines, or automated takedown for high-risk synthetic videos. Regulation must clearly define the obligations for platforms and creators.

6. **Limited Focus on Gendered Harms and Vulnerable Groups**

   As recent reporting indicates, women and marginalised persons face disproportionate risk from deepfake harassment, non-consensual image manipulation, "nudify" apps, etc. The current framework lacks targeted protections for such vulnerabilities. The process of obtaining justice is lengthy, bureaucratic, and often ineffective.

PROPOSED FRAMEWORK FOR LEGAL REGULATIONS IN INDIA.

Given the gaps and risks identified, the following framework is proposed for India to regulate deepfake AI effectively. This framework would ideally be provided through a standalone statute (or an amendment/Part within the BNS / BNSS / BSA structure), focusing specifically on synthetic media, deepfakes, and AI-generated content.

The objections of the same are as follows: -

- To criminalise malicious generation, dissemination, and use of deepfake / synthetic media without consent or for wrongful purposes.
- To mandate platform transparency, traceability, watermarking / provenance labelling of synthetic media.
- To strengthen evidentiary standards for authentication, ensure rapid takedown and secure preservation of evidence.
- To protect individuals' personality, image, voice, artistic identity, and reputation.
- To deter large-scale political manipulation, misinformation, and foreign influence campaigns.
- To enable effective redress for victims (removal, compensation, criminal sanctions).

PROPOSED LEGAL PROVISIONS: - DEEPFAKE AND SYNTHETIC MEDIA REGULATIONS ACT

1. Definition

- Define *"synthetic media"* or *"deepfake"* comprehensively to include any video, audio, image, or multimedia content that is generated, modified, or materially altered using artificial intelligence, machine learning, or generative technologies.
- The definition should cover content that depicts persons, voices, actions, or events that were not originally recorded, or that substantially manipulates authentic content so as to misrepresent reality.

2. Offence: Malicious Creation and Distribution of Deepfakes

2.1 The creation, publication, or distribution of deepfake or synthetic media content shall constitute a criminal offence where such activity is undertaken with malicious or unlawful intent. This includes impersonating a real person without their consent for the purposes of defamation, harassment, fraud, or disturbance of public order; portraying public officials or authorities as making statements or engaging in acts they did not perform with the intent to mislead the public, manipulate electoral processes, incite violence, or undermine democratic institutions; producing or circulating non-consensual intimate or sexually explicit synthetic content, including voice cloning or impersonation that targets private individuals; and engaging in repeated, organised, or commercial-scale creation or dissemination of deepfakes for defamation, scams, or financial fraud.

2.2 Penalties should be proportionate and graded based on intent, harm caused, scale of dissemination, and recurrence of the offence.

3. Civil Remedies, Injunctions, and Compensation

- Provide victims with the right to seek urgent interim and final injunctions for removal or blocking of deepfake content.
- Enable claims for statutory damages and compensation for reputational, emotional, or financial harm.
- Recognise misuse of an individual's likeness or voice as a civil wrong warranting injunctive and compensatory relief.

4. Platform Liability and Intermediary Obligations

- Mandate online platforms and intermediaries to deploy reasonable detection and mitigation mechanisms for synthetic media.

- Require expeditious takedown upon receipt of a credible complaint, within defined timelines (e.g., 24–36 hours for high-impact or harmful deepfakes).
- Oblige platforms to preserve relevant metadata, logs, and source information for investigative and evidentiary purposes.
- Impose periodic transparency and compliance reporting, including quarterly disclosures of complaints received and actions taken.

5. Labelling, Watermarking, and Metadata Requirements

- Require all synthetic or AI-generated content to carry a clear and conspicuous label or watermark indicating that it is "AI-generated" or "synthetic media."
- Prescribe minimum technical standards, such as visible watermarks covering a defined portion of images or videos, and embedded metadata tags in the initial frames of video or the first segment of audio playback.
- Ensure labelling standards are uniform and easily recognisable by users.

6. Forensic and Evidentiary Standards

- Establish a statutory framework for forensic verification of synthetic media, including accreditation of certified forensic laboratories.
- Lay down standards for provenance tracking, metadata preservation, and chain-of-custody for digital evidence.
- Provide for evidentiary presumptions whereby content identified as a deepfake by an independent certified forensic authority shifts the burden of proof to the uploader to establish authenticity.

7. Protection for Artistic Expression and Creators

- Safeguard artists and creators against unauthorised use of their likeness, voice, or distinctive artistic style through synthetic media.
- Treat such misuse as an actionable infringement, including violations of moral rights, with remedies for takedown, compensation, and attribution where appropriate.
- Establish accessible reporting and redressal mechanisms for affected creators.

8. Awareness, Education, and Digital Literacy

- Mandate government-led and public–private initiatives to promote awareness about deepfakes and synthetic media.
- Integrate digital literacy and media verification programs, with special focus on vulnerable groups such as women, youth, and senior citizens.

9. **Regulatory Oversight and Institutional Mechanism**
    - Constitute a dedicated statutory authority, such as a *Synthetic Media Regulatory Authority*, to oversee implementation of the Act.
    - Empower the authority to set and update labelling standards, certify detection tools and forensic labs, audit platform compliance, and maintain a central registry of reported synthetic media incidents.

CONSTITUTIONAL AND STATUTORY COMPATIBILITY: ALIGNMENT WITH THE INDIAN LEGAL FRAMEWORK

In recommending this normative framework, it is necessary to align with India's existing constitutional protections and statutory reforms.

1. **Freedom of Speech (Article 19)**

    The proposed legislation must respect the fundamental right to free speech and legitimate creative expression, especially for satire, parody, legitimate commentary, artistic use, and public interest uses. Accordingly, the definition of "malicious deepfake" must be carefully drafted to exempt bona fide satire, parody, political criticism, and transformative uses. Reasonable exceptions should be included (e.g. parody / artistic transformation with no intent to defraud/mislead; public interest disclosures). A balancing test between freedom of expression and protection of reputation / public order is necessary.

2. **Right to Life and Personal Liberty (Article 21) and Personality Rights**

    The victims' right to dignity, reputation, privacy, and bodily integrity is protected under Article 21 jurisprudence. The proposed statutory remedies (injunction, removal, damages) and procedural safeguards must ensure due process. The criminal offence must be backed by clear mens rea (intent to defraud/defame/impersonate / public order/election interference), to prevent over-broad chilling of legitimate expression.

3. **Criminal Offences under Bharatiya Nyaya Sanhita (BNS)**

    The Bharatiya Nyaya Sanhita (the reformed criminal law) already provides for offences relating to impersonation, forgery, defamation, identity fraud, cyber offences, etc. However, the new deepfake offence should complement—not duplicate—existing provisions. The deepfake offence should be distinct, with elements tailored to synthetic

media generation, manipulation, and large-scale dissemination with the intent to mislead. This will provide clarity rather than shoehorning deepfake cases into generic provisions.

4. **Evidentiary Reform under Bharatiya Sakshya Adhiniyam**

   The BSA reforms the law of evidence; accordingly, the statutory forensic standards, admissibility of synthetic media, burden-shifting, expert forensic certification, and authentication protocol must be incorporated. The proposed statute can integrate with the BSA, providing a schedule for forensic labs, registration, and chain-of-custody rules for synthetic content.

IMPLICATIONS FOR STAKEHOLDERS AND BROADER SOCIETAL BENEFITS

For Individuals and Victims

Victims of non-consensual deepfake pornography, political impersonation, identity fraud, and defamation will have a direct statutory pathway for urgent relief, takedown, and compensation. Artists, performers, and public figures will have protection over their voice, likeness, and creative identity, reducing misuse and impersonation. Ordinary citizens will benefit from improved trust in the authenticity of media, clearer labelling, and stronger deterrence against malicious impersonation or fake content.

For Democratic Institutions and Elections

A statutory regime will strengthen safeguards against political misinformation, election manipulation through synthetic videos or audio impersonation, foreign interference, and fake campaigning. The law will incentivise platforms to invest in detection, traceability, and transparency, thereby mitigating viral deepfake misinformation proactively.

For the Platforms and Technology Industry

Legal certainty will allow platforms to build robust compliance mechanisms (detection, labelling, transparency reports). Regulation will foster the responsible development of generative AI models and content-generation tools, including built-in watermarking, provenance tagging, and detection APIs. Certified forensic labs and third-party detection ecosystems will emerge, supporting accountability

POTENTIAL CHALLENGES AND OPPOSING PERSPECTIVES

While the proposed framework is necessary, it is not without challenges. Some of these include:

1. **Balancing Free Speech and Over-Regulation**
   There is a risk that broad definitions could chill legitimate expression, satire, political speech, or artistic experimentation. To counter this, the statute must be precisely worded, include reasonable carve-outs (satire, parody, public interest disclosure), and provide judicial oversight for takedown or injunction orders.
2. **Technical Complexity and Efficacy of Detection**
   Deepfake creation and detection are evolving rapidly. Over-reliance on detection tools may produce false positives or negatives. The statute must allow flexibility for new detection methods, periodic review, and standards for certification of forensic labs.
3. **Cross-Border and Jurisdictional Issues**
   Many deepfakes originate outside India, hosted on foreign platforms or uploaded anonymously. Enforcement and takedown pose jurisdictional challenges. The law should include provisions for cross-border cooperation, mutual legal assistance, and obligations of intermediaries under Indian jurisdiction.
4. **Resource Constraints and Judicial Capacity**
   Courts and law-enforcement agencies may be resource-constrained; forensic labs may need capacity building. The statute should allocate resources for certified labs, training, and quick-response teams.
5. **Implementation and Compliance Burden on Platforms**
   Platforms may find compliance burdensome. The law should be reasonable: smaller platforms may be exempt from certain obligations or provided with graduated compliance paths. Transparent guidance and regulatory sandboxes can help.

CONCLUSION

The proliferation of deepfake AI and synthetic media represents one of the most significant challenges confronting contemporary internet society. As the fidelity, accessibility, and reach of deepfake generation accelerate, individuals' reputations, democratic discourse, electoral processes, artists' creative rights, and social trust are increasingly vulnerable. In India, while the fundamentals are present—constitutional protections for free speech and dignity, recently

reformed criminal and evidentiary statutes—there is no dedicated legal framework addressing deepfakes comprehensively.

This paper has highlighted illustrative misuse incidents (both in India and globally), analysed the inadequacies of current law, drawn lessons from international developments (notably Denmark's proposed legislation), and proposed a detailed statutory framework for a Deepfake and Synthetic Media Regulation Act. Such regulation would criminalise malicious deepfake creation/distribution, mandate labelling and watermarking, strengthen forensic standards and platform accountability, provide victims with swift redress, and ultimately restore trust in digital media.

Legislators, policymakers, civil society, and the legal fraternity must prioritise the drafting and enactment of a bespoke deepfake law in India. Without it, the harms posed by synthetic media will grow, and society's capacity to self-govern, verify reality, and uphold democratic accountability will erode.