WHEN REALITY BREAKS: DEEPFAKES, DEFAMATION, FRAUD, AND THE UNRAVELLING OF PERSONALITY RIGHTS IN INDIA'S REGULATORY DARK ZONE

Kavya Sharma, KPMSOL NMIMS School of Law, Mumbai

Anubhav Sharma, KPMSOL NMIMS School of Law, Mumbai

ABSTRACT

Deepfakes pose significant challenges to misinformation and societal norms like truth and trust in India. The cultural emphasis on honor and reputation makes the population particularly sensitive to the negative impacts of deepfakes, which have led to defamation, financial fraud, scams, and heightened rates of suicide and violence, especially against women and certain communities. The lack of an effective legal framework to protect individual rights has only exacerbated these issues. Financial losses due to deepfakes are projected to exceed ₹70,000 crore by 2025, with a staggering increase in cybercrime rates related to this technology.

This paper explores how deepfakes undermine basic doctrines of defamation, fraud, and evidentiary reliability while proposing a personality rights-centered regulatory framework aligned with Article 21's protections of dignity, privacy, and reputation. This approach aims to balance innovation and freedom of expression with necessary protections and accountability measures. Ultimately, the study underscores the urgent need to reform India's legal architecture to address the human costs associated with synthetic media.

1) INTRODUCTION

Deepfakes are no longer just something that was solely on the fringe of the internet; deepfakes have become the main way people deceive one another. Deepfakes can be used to manipulate an entire election; create false identities and create an "alternative" trustworthy record of what a person said or did. So far at least 38 countries with approximately 3.8 billion people have had some form of deepfake related incidents during competitive elections across the globe, with India and several other large democracies witnessing the fabrics of AI-generated robocalls and synthetic media being used to generate false narratives, suppress voters and heighten the levels of political polarisation in addition to the diminishing public trust in democratic institutions. In India, the creation of synthetic representations has created a "dark zone" where the law has not yet adapted to AI-generated defamation and fraud, as there is a very weak legal framework designed to protect an individual's reputation, privacy, and personality. As the dark zone continues to grow, so does cybercrime related to deepfakes; research projects a growth in deepfake-related cybercrime of approximately 550% since 2019 and expects to see more than

₹70,000 crore (approximately $10 billion) in losses due to fraud by 2025. However, these numbers do not depict the human toll that so many individuals experience. A single non-consensual deepfake has the power to ruin an individual family's honour and create vigilante or honour-based violence upon the targeted individual.

India does not have a specific deepfake statute, codified personality-rights code, or any mandated detection infrastructure like those increasingly deployed in the US/EU. Thus, non-consensual sexual deepfakes, cross-border culpability, and mass political manipulation rely on generic offences of identity theft and defamation. This paper approaches deepfakes as a constitutional and human-rights issue: personal liberty, reputation, equality, and dignity have been hit, especially concerning women and minorities. It contends that a robust Indian response will necessarily link evidence, personhood, and platform governance in order to protect these constitutional values from synthetic-media harms.

2) LITERATURE REVIEW

Literature increasingly treats deepfakes as an epistemic threat rather than a technical novelty. UNESCO establishes them as a “crisis of knowing” that it weakens the confidence in audiovisual evidence, while philosophers Luciano Floridi and Brian Skyrms argue that deepfakes diminish the information-carrying capacity of video, amplify false beliefs, and enable the "liar's dividend," allowing genuine evidence to be dismissed as fake.[1]

2,1 Global and Electoral Impacts

Deepfakes have affected 38 countries (3.8 billion people) in elections since 2021, with 92% of incidents spread via social media. Reviews highlight risks to privacy and democracy, noting that detection methods lag behind rapid impersonation.[2]

2.2 Indian Legal Scholarship

Indian law addresses traditional privacy but not AI-specific harms like non-consensual deepfake creation. Section 66 of the IT Act is criticized for oversimplifying deepfakes as mere impersonation. India also lacks mandatory detection or watermarking systems, making it reactive compared to the US and EU.[3]

2.3 Personality Rights Evolution

Personality rights protect celebrities under Article 21, as seen in recent deepfake injunctions. However, issues remain, such as a focus on commercial interests, neglect of ordinary victims, and challenges in addressing non-economic harms

3) RESEARCH GAP

Literature maps harms but neglects India's detection software deficit, Section 66's inadequacy for synthetic anonymity, and deepfakes' amplified cultural devastation in conservative societies like India.[4]

[1] UNESCO, Deepfakes and the Crisis of Knowing, https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing (last visited Jan. 7, 2026).

[2] Surfshark, Election-Related Deepfakes, https://surfshark.com/research/chart/election-related- deepfakes (published Jul. 29, 2025; last visited Jan. 7, 2026)

[3] Tanmaya Nirmal, Deepfakes in India: Legal Landscape, Judicial Responses and a Practical Playbook for Enforcement, NeGD, https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/ (posted Sept. 29, 2025; last visited Jan. 7, 2026)

[4] Juhi Chandel & Manisha Kundu, AI-Generated Deepfakes and the Legal Vacuum in India: A Constitutional Analysis of Privacy, Consent, and Digital Harm Under Article 21, 10 IJRTI 850 (Nov.2025), https://www.ijrti.org/papers/IJRTI2511099.pdf (last visited Jan. 7, 2026).

4) RESEARCH OBJECTIVES

1. To analyse deepfakes' impact on defamation, fraud, evidentiary reliability, and IT Act Section 66 limitations in India, including the absence of dedicated detection software unlike global standards.[5]

2. To assess regulatory inadequacies under IT laws, criminal provisions, and personality rights, mapping gaps in culprit attribution amid encrypted generation and cross border servers[6].

3. To analyze how deepfake technology violates personality rights in India, leading to commercial exploitation, and to evaluate the gaps in the current legal framework that fail to prevent such exploitation, and to propose the need for focused legislative reform.

5) RESEARCH QUESTIONS

1. How do deepfakes undermine Indian defamation, fraud law, and the evidentiary value of audiovisual material under the IT Act?

2. Why do India's IT, criminal, and personality rights laws fail to effectively regulate AI impersonation and cross-border offenders?

3. Do existing laws adequately address the social and reputational harm caused by deepfakes in India, or are personality-centred reforms required?

6) RESEARCH METHODOLOGY

6.1 Qualitative Analysis- This study employs **qualitative doctrinal and socio-legal methods** to examine deepfake harms, legal frameworks, and policy gaps in India. Primary data collection involved systematic review of secondary sources including peer-reviewed papers, legal commentaries, government advisories (MeitY, PIB), judicial orders, and credible news reports (2023–2026) sourced via keyword searches ("deepfake India suicide", "synthetic intimate imagery honour", "deepfake BNS defamation"). **Thematic analysis** identified harm pathways (reputation destruction, honour-based stigma, suicide ideation),

[5] Don Fallis, The Epistemic Threat of Deepfakes, 34 PHILOS. & TECH. 623 (2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC7406872/ (last visited Jan. 7, 2026).

[6] Rising Menace of Deepfakes with the Help of AI: Legal Implications in India, IJIRL (May 2024), https://ijirl.com/wp-content/uploads/2024/05/RISING-MENACE-OF-DEEPFAKES-WITH-THE-HELP-OF-AI-LEGAL-IMPLICATIONS-IN-INDIA.pdf (last visited Jan. 7, 2026)

doctrinal applicability (BNS §356, IT Act

§§66C–67A, DPDP), and institutional weaknesses, with case studies (Faridabad, Ghaziabad, Rashmika Mandanna) triangulated for pattern validation. Normative recommendations emerged from comparative analysis of Indian (MeitY advisories) and global (US/EU) regulatory models.

6.2 Quantitative Analysis- Secondary quantitative data was extracted from existing surveys and official statistics to establish prevalence and scale. Key metrics include: McAfee survey (75% Indians exposed to deepfakes, 38% faced scams); global deepfake susceptibility rankings (India #6); cybercrime surge (550% since 2019); projected fraud losses (₹70,000 crore by 2025); and NCRB/IC3 student suicide figures (13,044 in 2022, 1 lakh+ 2013–22). These were descriptively analysed for correlations between deepfake exposure and vulnerability markers (student suicides, honour-risk contexts) without inferential statistics due to data limitations. Sources were selected for recency and credibility, cross-verified across multiple reports.

6.3 Limitations: No primary data collection (surveys/interviews) due to ethical constraints around victim privacy in suicide/honour cases; quantitative reliance on aggregated secondary statistics may understate prevalence (65% under-reporting); qualitative focus risks selection bias despite triangulation. Future research could incorporate anonymised victim surveys and forensic deepfake datasets. This mixed secondary approach suits rapid academic analysis of an emerging law-technology intersection for a law student.

7) DISCUSSION

Deepfakes in India have rapidly become a tool for harassment and reputational violence, particularly affecting women and young people. These manipulative images and videos exploit existing gender, caste, and age hierarchies, leading to acute shame, anxiety, and even suicidal thoughts in victims, especially when such content spreads in close-knit communities like family WhatsApp groups or colleges.[7]

[7] National Herald India, India Sixth Most Susceptible Country to Deepfakes: Can Laws Tackle the Menace?, https://www.nationalheraldindia.com/science-tech/india-sixth-most-susceptible-country-to-deepfakes- can-laws-tackle-the-menace (last visited Jan. 7, 2026)

Victims often experience depression and social withdrawal, and families may suppress complaints to protect their honor, echoing dynamics seen in honour-based crimes. Recent incidents illustrate the grave consequences of deepfake harassment, such as the 2025 suicide of Rahul Bharti, who faced blackmail with AI-generated content, highlighting the severe emotional distress induced by these attacks. A survey shows that over 75% of Indian users encountered deepfake content in the past year, with a significant number experiencing scams. The intersection of digital humiliation and suicidality remains a serious concern, reflecting the urgent need for awareness and interventions against these threat**s.**[8]

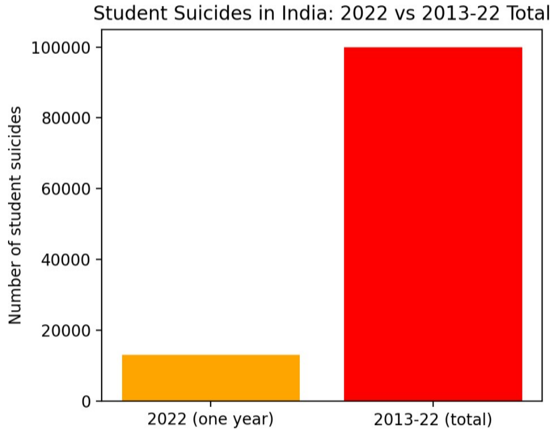

Figure 1.1 (Student suicides: 2022 vs 2013–22 total)

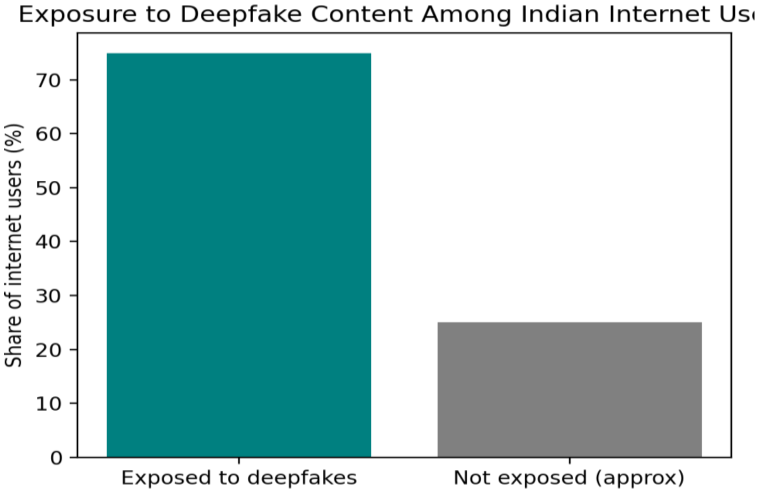

Figure 1.2 -(Exposure to deepfakes among Indian internet users)

[8] IJLSSS, Deepfakes as a Weapon of Gendered Terror: Non-Consensual Synthetic Intimacy and the Systematic Harassment of Women and Marginalised Communities, https://ijlsss.com/deepfakes-as-a-weapon-of-gendered-terror-non-consensual-synthetic-intimacy-and-the-systematic-harassment-of-women-and-marginalised-communities/ (last visited Jan. 7, 2026)

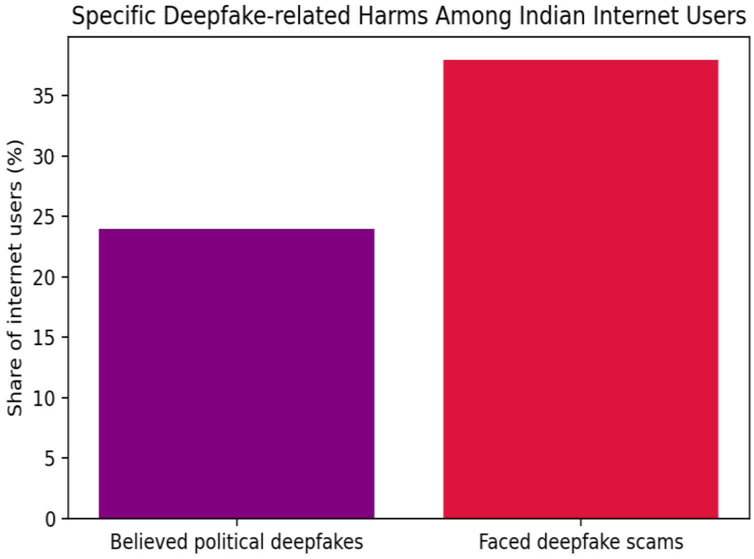

Figure 1.3- Specific deepfake-related harms among Indian internet users

7.1 Personal reputation and defamation

Personal reputation is the main harm caused by deepfake abuse. Deepfakes create false evidence of immoral conduct that can be easily shared, making recovery of one's reputation difficult. Victims, particularly women, face severe consequences such as being labeled "characterless," losing relationships, or dropping out of education or work. They often live in fear that potential employers or family members will discover harmful content. Reputational harm can extend to families, as seen in cases like Faridabad. Defamation law, as outlined in the Bharatiya Nyaya Sanhita 2023, addresses this with provisions for synthetic images and videos that damage a person's standing. While scholarly analysis suggests that these laws may apply to AI-generated defamation, challenges remain regarding authorship, malice, and liability, and civil actions are often slow compared to the rapid spread of viral content.[9]

7.2 Legal framework and reporting mechanisms

Deepfakes intersect with various legal areas, such as defamation, privacy, and cybercrime, rather than being regulated by a single law. The IT Act 2000 includes provisions against identity theft (Sections 66C, 66D) and privacy violations (Section 66E), as well as laws against the

[9] IJCRT, Reputation and Defamation in Deepfake Era, https://ijcrt.org/papers/IJCRT2405231.pdf (May 23, 2024)

distribution of obscene content (Sections 67, 67A). General criminal laws apply in cases of blackmail or self-harm. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 require platforms to have clear policies and remove unlawful content within 36 hours of notice to maintain safe-harbour protections.

Courts increasingly invoke personality and privacy rights to restrain deepfake misuse of image and voice, particularly for public figures. Injunctions against morphed videos and unauthorised exploitation of likeness are grounded in the right to privacy and developing publicity rights, reflecting judicial recognition that AI-manipulated media can gravely injure dignity and autonomy. The Digital Personal Data Protection Act 2023 adds a data-protection layer by regulating the processing of personal and biometric data used to train or generate deepfakes and offering grounds to challenge unauthorised or harmful processing. However, responses remain fragmented and largely reactive, often placing heavy procedural burdens on already traumatised victims.

India's cyber-reporting infrastructure is essential, with the National Cyber Crime Reporting Portal (cybercrime.gov.in) serving as a unified platform for complaints on issues like cyberbullying, identity theft, and more. It has specific modules for crimes against women and children, along with links to report abuse to social media platforms. For financial fraud, the helpline 1930 allows for rapid reporting to help trace funds. State portals, like the Maharashtra Cyber Portal, and initiatives like Sanchar Saathi assist users in reporting threats and securing mobile connections. Official guidance advises a layered response: report to the platform, file a complaint on the cyber portal with evidence, and lodge an FIR with local police for serious threats.[10]

7.3 Personality Rights

The Delhi High Court has issued orders to protect the personality rights of celebrities and public figures from unauthorized commercial use. These individuals sought legal action against the misuse of their names, photos, and AI-generated content. The court has granted interim injunctions and John Doe orders to remove unauthorized content and prevent misuse of their personas. This highlights the importance of understanding personality rights, especially

[10] Cybercrime.gov.in, https://cybercrime.gov.in/Webform/Accept.aspx (last visited Jan. 7, 2026).

concerning AI technologies like Deepfakes that exploit public figures for commercial gain.[11]

Personality rights protect an individual from unauthorized use of their name, voice, image, and likeness for unsanctioned commercial use. The concept of personality rights is derived from two primary components –

7.3.1 Publicity Rights – These rights primarily deal with the safeguards against the commercial use of personality traits such as name, image, signature, etc. In the case of celebrities, these personality rights also have an **economic value** attached to them, as unauthorized usage involves the goodwill of such a person to sell a product or to generate revenue out of it.

7.3.2 Right to Privacy – Privacy rights, unlike the commercial focus of publicity rights, protect individuals, even non-celebrities, from harm irrespective of any economic or commercial aspect of it, such as unwanted exposure, right to be let alone, defamation, sextortion, etc. This prevents misrepresentation of personal details. In India right to privacy was recognized by the Supreme Court in the 2017 Puttaswamy judgement, where the court viewed the right to privacy as an extension of dignity and personal liberty.[12]

7.4 IMPACT OF DEEPFAKE ON PERSONALITY RIGHTS AND RISE IN COMMERCIAL EXPLOITATION

Deepfakes are becoming more commonly used to fabricate people's images, voices, likenesses, or personas through deep learning techniques. These manipulated media can create a false reality, such as face swapping, where a celebrity appears to make commercial endorsements, or voice cloning for fake speeches or fraudulent calls.

Deepfake-related cyber offences have increased by 550% since 2019, with projected losses worth 70,000 crore rupees in the year 2025 as per the “Digital Deception Epidemic: 2024 Report on Deepfake Fraud’s Toll on IndiaDeepfakes have also been reported as one of the 10

[11] IJLMH, Personality Rights in India: Available Safeguards Against Exploitation, https://ijlmh.com/paper/personality-rights-in-india-available-safeguards-against-exploitation/ (last visited Jan. 7, 2026); Drishti IAS, Personality Rights, https://www.drishtiias.com/daily- updates/daily-news-analysis/personality-rights-2 (last visited Jan. 7, 2026)

[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

major global risks as per the 2024 World Economic Forum's Global Risks Report[13].

The swift dissemination of information on social media presents challenges because user anonymity complicates the verification of content sources. Consequently, many individuals may unwillingly become vulnerable to deceptive information before the fraud is identified. This can result in people believing such content without having any knowledge of its truthfulness. There are several cases where the use of Deepfakes has resulted in commercial exploitation.

Ankur Warikoo & Anr. Vs John Doe & Ors.[14] – AI-generated deepfake videos of influencer Ankur Warikoo, founder of Zaan Web Veda, were created to mislead investors by promoting fraudulent WhatsApp groups offering deceptive stock market advice. These videos circulated on social media, resulting in significant financial losses for individuals who invested through dubious apps. Warikoo took legal action in the Delhi High Court against the unidentified creators, claiming that the deepfakes harmed his company's interests as well as his personal reputation. The court issued injunctions for the removal of such content, but despite identification by cybercrime authorities, some platforms continued to display it, highlighting the risks of deepfakes in harming personality rights and enabling fraud.

Ravi Shankar v John Doe(s) / Ashok Kumar(s) & Ors. Renowned spiritual guru Gurudev Sri Sri Ravi Shankar filed a case in the Delhi High Court against John Doe for publishing deepfake content using his likeness to falsely promote ayurvedic medicines with exaggerated claims. The plaintiff argued that his voice, image, and reputation are protected as personality rights under articles 19(1)(a) and 21. The court issued orders preventing any unauthorized commercial use of his persona, highlighting the risks of deepfakes misleading the public.[15]

In another incident, two individuals a woman and a retired employee who were residents of Bengaluru fell victim to a scam involving deepfake videos of Infosys co-founder Narayan Murthy and Reliance Industries chairman Mukesh Ambani. These videos showed the well-

[13] ET Edge Insights, India to Lose Rs 70,000 Crore in 2025 Due to Deepfake Fraud: Study, https://etedge-insights.com/trending/india-to-lose-rs70000-crore-in-2025-due-to-deepfake-fraud-study/ (2024); IIPRD, The Mirage of Fame: Deepfakes, AI, and Evolving Jurisprudence on Personality Rights, https://www.iiprd.com/the-mirage-of-fame-deepfakes-ai-and-evolving-jurisprudence-on-personality-rights/ (2024)

[14] Ankur Warikoo and Another v John Doe and Others, 2025 SCC OnLine Del 3727.

[15] SCC Online, Delhi HC Grants Interim Relief to Sri Ravi Shankar in Personality Rights Case, https://www.scconline.com/blog/post/2025/10/07/del-hc-grants-interim-relief-to-sri-ravi-shankar-in-personality-rights-case/ (Oct. 7, 2025). Ravi Shankar v. John Doe, Delhi High Ct. (2025)

known businessmen promoting fraudulent trading platforms that promised significant profits on investments. The perpetrator created these deepfake videos using actual recordings of the businessmen taken from company addresses, stakeholder meetings, or public events.

The modus operandi was the same; the victims were asked to make investments by providing them with fake links to websites and asking them to invest their money in fake bank accounts, promising substantial returns, but they received no such returns, and the money was scammed. Both these incidents resulted in a collective scam of approximately 95 lakhs[16].

7.5 LEGAL FRAMEWORK

There is currently no uniform legislation in India that regulates the use of deepfakes. So far, Indian courts have relied on the right to privacy under Article 21, the Copyright Act, the Trademark Act, and judicial doctrines such as passing off to provide relief to victims. However, there are significant gaps in these legal frameworks. For example, the Copyright Act extends protections only to "performers," excluding non-performers, and the Trademark Act does not protect marks for non-commercial use on goods or websites that have not yet been registered.[17]

Due to a lack of legal clarity, there are jurisdictional gaps in how courts handle misuse cases. Only the High Courts of Delhi, Mumbai, Calcutta, and Madras have original civil jurisdiction, allowing swift injunctions for those within their reach. In contrast, individuals outside these areas must go through district courts, prolonging the process. This delay is especially problematic for ordinary citizens, as information spreads rapidly. Moreover, many courts lack the necessary technological expertise to address complex issues like deepfake generation using GANs and deep learning techniques.

The issue of attribution in finding out the original generator and decrypting information about it, and the problem of deepfake generation across the border, beyond the jurisdiction of Indian

[16] Times of India, Bengaluru Residents Duped of Rs 95 Lakh by Deepfake Videos of Narayana Murthy and Mukesh Ambani, https://timesofindia.indiatimes.com/technology/tech-news/bengaluru-residents-duped-of-rs-95- lakh-by-deepfake-videos-of-narayana-murthy-and-mukesh-ambani/articleshow/114955868.cms (2024)

[17] Khurana & Khurana, Personality Rights in Peril: Addressing AI-Generated Cloning Through Indian Legal Frameworks, https://www.khuranaandkhurana.com/personality-rights-in-peril-addressing-ai-generated-cloning-through-indian-legal-frameworks (last visited Jan. 7, 2026).

courts require clear framework to strengthen cross-border enforcement[18].

The proposed amendments to the **Information Technology Act 2000** include updates to Section 66D to address deepfakes that use someone's likeness for fraud or defamation, while Section 66E would be revised to encompass privacy violations stemming from deepfakes. Additionally, Section 79 should mandate intermediaries to resolve deepfake complaints within 24 to 36 hours in order to maintain their safe harbour protection. Under the **Bhartiya Nyaya Sanhita**, amendments are necessary to combat AI cheating via deepfakes, particularly in scams similar to those affecting Bengaluru residents, with Section 353 needing to explicitly include deepfakes as a means to propagate false information and incite violence. The **Digital Personal Data Protection Act 2023** should affirm that an individual's voice, likeness, and other identity traits are classified as personal data, allowing individuals the right to sue for unauthorized use in AI-generated content like deepfakes. Finally, the **Copyright Act 1957** should be extended to protect the rights of non-performers against unauthorized use of their likeness, while the **Trademark Act 1999** needs to address the implications of deepfake technology on trademarks and incorporate doctrines of passing off to ensure uniformity across legal jurisdictions.

7.6 TOWARDS A UNIFIED LEGISLATION FOR DEEPFAKE REGULATION

To effectively address deepfake issues, there should be a single piece of legislation that governs the ethical use of deep learning techniques, allowing for the swift removal of unauthorized content. This law should grant individuals rights over their likeness and provide mechanismsfor self-removal from digital platforms. In India, establishing tech-benches for takedowns could help prevent the rapid spread of such content. We can look to Denmark's Deepfake Regulation, which gives citizens’ rights over their voice and likeness, as a model. Additionally, a UN-backed cybercrime treaty is needed to address cross-border deepfake offenses.

Despite these regulations, significant loopholes still exist. For example, the law in Denmark grants copyright to individuals over their persona; however, it does not address the unethical use of deepfakes by those individuals themselves, such as for inciting communal violence. Granting property rights over one's personality could create a situation where an average

[18] IP & Legal Filings, Personality Rights in the Era of Deepfakes and Synthetic Media, https://www.ipandlegalfilings.com/personality-rights-in-the-era-of-deepfakes-and-synthetic-media/ (last visited Jan. 7, 2026).

person would need to charge a licensing fee to have their photo removed. Additionally, for copyright to apply, there must be a unique creative expression involved.

8) RECOMMENDATION AND WAY FORWARD

8.1 Recognition of Deepfakes as a Separate Harm

Indian law should recognise deepfakes as a distinct digital harm. A specific offence for non consensual synthetic media and malicious impersonation would improve clarity and deterrence, with enhanced penalties where minors are involved, conduct is repeated, or serious psychological harm results.

8.2 Applicability of Existing Laws

It must be expressly clarified that the Bharatiya Nyaya Sanhita, the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023 apply to digitally generated images, voice and likeness, including unauthorised use for training or reproduction.

8.3 Platform and Intermediary Responsibility

Intermediary rules should require timely takedown of harmful deepfakes, clear labelling of synthetic content and accessible grievance redressal mechanisms. Platforms that repeatedly fail to act despite notice should face proportionate liability.

8.4 Institutional Support Mechanisms

A specialised national body can assist courts and law enforcement through forensic expertise, coordination and standard setting. Fast track mechanisms for synthetic media harms can enable urgent takedowns and interim relief for victims.

8.5 Rights Based Victim Protection

Recognising a right to authentic digital identity within privacy and personality rights would place dignity and reputation at the centre of deepfake regulation. Compensation mechanisms can provide timely relief where harm is severe.

8.6 Operational Reforms

The National Cyber Crime Reporting Portal and the 1930 helpline should include a dedicated deepfake reporting category with standardised evidence requirements and rapid coordination with cyber and telecom authorities

8.7 Psychosocial and Legal Support

Legal remedies must be linked with counselling and legal aid services, particularly for women, students and marginalised communities facing stigma or retaliation

8.8 Norm Building Beyond Law

India has evolved from experimenting with Deepfakes to utilizing them for systematic violence through digital media. Victims often face humiliation, shame, and even suicidal thoughts due to non-consensual synthetic images that exploit existing social hierarchies like caste, gender, and honour. Non-consensual intimate imagery and impersonation deepfakes pose serious threats to reputation, dignity, and family honour in India. These convincing false audiovisual materials are easily accepted in close-knit communities, disproportionately harming vulnerable individuals. This paper argues for recognizing deepfakes as a distinct digital harm linked to personal honour and reputation, advocating for specific legal provisions to address the creation and distribution of non-consensual imagery. Clear guidance on legal remedies under the IT Act and defamation laws is necessary.

Moreover, stronger responsibilities should be placed on AI developers and digital platforms to detect and respond to deepfake content. Investing in specialized regulatory bodies, forensic expertise, and victim support mechanisms can help shift India toward prioritizing dignity and personal reputation over reactive crisis responses.