Page 1550 - 1567 **DOI:** *https://doij.org/10.10000/IJLMH.1111413*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 1

2026

Stolen Faces, Borrowed Voices: The Legal Imperative for Regulating Deepfake in India

PRIYANSHU YADAV[1]

ABSTRACT

The expansion of Generative Adversarial Networks, or GANs, has created space for new sort of synthetic media known as deepfakes. Our long held conviction that anything you witness with your own eyes must be true is challenged by these audio and video recordings, which appear so real that they make it difficult to distinguish between reality and fiction. This study focuses closely at the legal and ethical repercussions of deepfake technology. Even though it has legitimate creative applications, particularly in fields like entertainment and cinema, it is also turning into a potent instrument for harming people by violating their privacy and undermining public confidence. Also it alerts people to a rising threat to India's democracy: the use of phony audio or video to disseminate misleading information and sway public opinion during elections.

This work focuses on how Indian courts are employing personality rights to combat personal data theft and digital impersonation by examining recent court rulings, such as those in the Anil Kapoor and Arijit Singh cases. It also takes a serious look at whether our current legislation the Information Technology Act, 2000 the Bharatiya Nyaya Sanhita and the Copyright Act are strong enough to deal with the difficulties deepfakes provide. This paper argues that although our present laws offer some scattered answers for things like cybercrime and defamation, they fall short in the matter of regulating the particular subject matter of AI generated identity theft and impersonation.

Keywords: *Deepfake Technology, Artificial Intelligence, Personality Rights, Cyber Law, and Disinformation*

I. THE ORIGIN AND WORKING PROCESS OF SYNTHETIC MEDIA

When fake and deep learning are combined, deepfake indicate a particular kind of AI technology.[2] Deepfakes use artificial intelligence to digitally alter faces in a video. This technology allows for the creation of highly lifelike recordings of people saying or acting in ways they never did before. [3].

[1] Author is a Student at University of Allahabad, Uttar Pradesh, India.

[2] Prajakta Pradhan, *AI Deepfakes. The Goose Is Cooked ?*, ILL. L. REV. BLOG(Oct. 4, 2020), https://illinoislawreview.org/blog/ai deepfakes/.

[3] Rituparna Bhattacharjee & Muskan Sharma, *Deepfake & Pornography: The Coming Crisis of Privacy and Consent*, 26 S. E. EUR. J. PUB. HEALTH (Supp. 2) 1196, 1196 (2025).

 [ISSN 2581-5369]

In an era of rapid digitization, there are gadgets all around us designed to make our lives easier. We ask voice activated assistants like Siri and Alexa for help in several ways, utilise Google Maps to drive us practically anywhere, and use search engines to find the information we need. The judicial system will inevitably be impacted by Al's invasion of every part of our lives. The interplay of AI technology, the decline in human intervention, and the constraints of the current legal framework, which was created specifically for humans, opens up discussion on how the current legal system might assess AI generated evidence[4].

A. Operational Mechanisms: GANs and LLMs

Large language models (LLM) and other generative AI systems provide new threats and opportunities to society. In 2014, Ian Goodfellow developed GANs. They use a generator and discriminator network that have been built against each other to create extremely realistic synthetic media that is very hard to distinguish from real recordings[5]. Some risks are rooted in the way humans interact with the technology, while others are related with the construction and operation of these models. These risks include privacy concerns, disinformation, and the issue of hallucinations[6]. Generative Adversarial Networks together with other deep learning models are at the forefront of the rapidly developing field of deepfake technology, which creates synthetic material including photos, videos, and sounds. Even human experts find it extremely difficult to find the authenticity of these models since they can nearly flawlessly replace the facial features of the original content with those of another person. Such rapid progress raises concern about the technology's potential for abuse, particularly when it is employed as a means of harassment, deception, and manipulation, endangering human rights[7].

B. The Dichotomy of Innovation and Malice

The astonishing growth of generative models in recent years has has sped up sharply in Deepfake's development. Applications of deepfake have demonstrated enormous promise in fields like advertising and filmmaking. However, its nefarious usage has has created intense ethical debate as well as serious security problems related to face forgeries. Not just that, facilitating the spread of misinformation and seriously endangering societal stability and

[4] Preeti Kushwah, *Evaluating the Evidential Value of Evidence Generated by AI*, 4 INDIAN J.L. & LEGAL RSCH. 1,1 (2022 2023).
[5] A. Shaji George, *Regulating Deepfakes to Protect Indian Elections*, 1 PARTNERS UNIVERSAL INNOVATIVE RESCH. PUB. 75,75 (2023), https://doi.org/10.5281/zenodo.10154619.
[6] Sandra Wachter, Brent Mittelstadt & Chris Russell, *Do large language models have a legal duty to tell the truth?*, 11 R. SOC'Y OPEN SCI., no. 8, art. 240197, at 1 (2024), https://doi.org/10.1098/rsos.240197.
[7] Emmanuel Pintelas & Ioannis E. Livieris, *Convolutional Neural Network Framework for Deepfake Detection: A Diffusion Based Approach*, 257 COMPUT. VIS. & IMG. UNDERSTANDING, 104375, at 1 (2025), https://doi.org/10.1016/j.cviu.2025.104375.

 [ISSN 2581-5369]

individual privacy, malicious Deepfakes also erode public confidence in digital media and institutions[8]. Deepfake poses a risk to identity verification, biometric privacy, and training data integrity[9]. By extracting a person's facial traits and projecting them onto a different body, deepfake technology significantly raises the danger of identity fraud by enabling plausible fake identities that jeopardize facial recognition-based systems used in banking, security, and access control[10]. By creating realistic, de identified medical films of illnesses, this technology can help medicine by providing doctors with crucial diagnostic information without jeopardizing patient privacy[11].

C. From Cheap Fakes to Hyper Realistic Forgeries

With deepfake technology, we enter a world of falsified existence, where artificial intelligence and fake learning are the norm. These days, the photos we take are edited and adjusted to look their finest. The background is colored appropriately, the skin tones are lighter, and the brightness function adds to the glitz. Better images can still be identified from the originals, but what about technology that produces an image that is so lifelike that it is impossible to tell them apart? The technology behind Deepfake is extremely intricate and beyond the comprehension of the average person. When it comes to mimicry and imitation, Deepfake technology is an expert. By focusing on a person's facial, gestural, and vocal patterns, deepfake technology creates a synthetic replica[12]. A digital forgery is not always a deepfake. People often refer to forgeries made by people with software editing tools known as cheap fakes. Altering images or audio visual content through speeding, slowing, pasting, or recontextualizing are examples of cheap fakes[13]. Deepfakes harm national security because hostile actors can use them to propagate disinformation, exploit social tensions, and create political upheaval, which has aroused major alarm among lawmakers[14].

---

[8] Chen Sun, Haiyang Sun, Zhiqing Guo, Yunfeng Diao, Liejun Wang, Dan Ma, Gaobo Yang & Keqin Li, *Diff Mark: Diffusion based robust watermark against Deepfakes*, 127 INFO. FUSION 103801, at 1 (2026), https://doi.org/10.1016/j.inffus.2025.103801.

[9] Wufeiyang Chen, *Deepfake Technology's Dual Nature: A Review of Security Risk Assessment and Defense Strategies*, *in* PROC. CONF MLA 2025 SYMP.: APPLIED ARTIF. INTEL. RSCH. 14, 15 (2025).

[10] *Id*. at 16.

[11] Weston Barker, *You Can Take It with You: An Argument for Establishing a North Carolina Postmortem Right of Publicity*, 24 N.C. J.L. & TECH. 1 (April 2023).

[12] Ivneet Kaur Walia, *Deepfake Technology as an Emerging Cyber Crime Facilitator: Analyzing the Necessity of Regulating Illusions and Unreal*, 51 INDIAN J. CRMINOLOGY 116,116 (2023).

[13] Hannah Smith & Katherine Mansted, WEAPONISED DEEP FAKES: NATIONAL SECURITY AND DEMOCRACY 5 (AUSTL. STRATEGIC POL'Y INST. 2020), https://www.jstor.org/stable/resrep25129.6.

[14] Aranya Nath & Sreelakshmi B., *Deepfakes on Copyright Law Inadequacy of Present Laws in Determining the Real Issues*, 15 INDIAN J.L. & JUST. 285,288 (March 2024).

 [ISSN 2581-5369]

II. JURIDICAL ANALYSIS OF PERSONALITY RIGHTS

In India, being a celebrity comprises way more than simply athletes and movie stars, it also includes influencers, spiritual leaders, and anybody whose image garners attention from the public and has monetary value[15]. Attacks using voice cloning have greater chance to target public personalities and celebrities than average people. Celebrities are more likely to be the main targets of voice cloning attacks, even though there is technology available to generate vocal dupes of private individuals. The AI bot requires a large number of sound clips of the victim's speech to be trained, and it is far simpler for criminals to locate celebrity voice recordings online. Beyond this, a fake film of a celebrity would gain way more attention than a video of a lesser known person if the tricksters are looking for widespread and disruptive influence or internet infamy[16].

A. Protection of Vocal Identity: The Arijit Singh Case

The majority of the early legal disputes against generative AI have been fought by celebrities who want to safeguard their priceless and painstakingly constructed public identities. One important court precedent in this area is the Bombay High Court's ruling in Arijit Singh v. Codible Ventures LLP[17], The plaintiff in this case, a well-known singer, requested an interim order for stopping the defendants who were developing and marketing intelligence systems to create synthetic audio samples of his speech. According to the Court's presumptive assessment, the injured party's distinguishable characteristics such as individuals identity, visual identity, voice, along with general persona are protected components of personality and publicity rights[18].

B. Safeguarding Persona: The Anil Kapoor Judgment

A wide-range of violations, including the specific usage of artificial intelligence in face morphing and voice cloning, were also brought before the Delhi High Court amid the 2023 case of Anil Kapoor v. Simply Life India[19], Court noted that any unauthorized and unlawful user can utilize, create, or mimic the persona of any celebrity through utilizing any technical means, with the use of artificial intelligence currently evolving into widely accessible[20]. Courts cannot neglect the misuse associated with celebrity's title, visual representation, or additional elements

[15] Prachi Bhardwaj, *What are Personality Rights? The rise of Celebrity Lawsuits Explained*, 2025 SCC OnLine Blog LME 8, at 2 (SCC OnLine, Oct. 21, 2025).
[16] Bryn Wells Edwards, *What's in a Voice? The Legal Implications of Voice Cloning*, 64 ARIZ. L. REV. 1213, 1223 (2022).
[17] Arijit Singh v. Codible Ventures LLP, 2024 SCC OnLine Bom 2445.
[18] *Id.* at ¶ 17.
[19] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914.
[20] *Id.* at ¶ 42.

 [ISSN 2581-5369]

of their identity, as the Delhi High Court correctly noted. Identity tarnishing, dilution, and blurring are examples of actions that are acknowledged as actionable wrongs that call for legal protection[21]. The Court further noted that even the unauthorized creation of ringtones, GIFs, or domain names for commercial gain amounts to a clear violation of personality rights[22].

C. Restraining Deepfake Abuse: The Aishwarya Rai Injunction

Likewise in Aishwarya Rai Bachchan v. Aishwaryaworld.com[23], in this case defendants employed AI techniques to illegally use the Plaintiff's name and photos without her authorization, resulting in financial loss along with damage to her goodwill, dignity, and reputation[24]. The Court reached the view that there was sufficient justification to issue an ex parte injunction[25]. With this decision, the defendants were expressly prohibited from utilizing the plaintiff's identity with the help of any technological means, such as Generative AI, Deepfakes, Face Morphing without her permission[26].

D. The Vulnerability of Public Personas: The Taylor Swift Incident

A recent viral outbreak of pornographic deepfake photos of Taylor Swift[27] created by artificial intelligence on the platform X brought this worldwide issue even more attention.A crucial point was raised when this incident became national news. Where social networking sites lacks the ability to protect among the most well-known women in the world, then whom do they have the capacity to protect ? We must recognize that celebrities are not the only threat. Their application go far beyond celebrities, they could be applied to harm reputation, privacy, and trust by targeting public personalities, private individuals, or entire communities[28].

III. GENDERED CYBER VIOLENCE AND NON CONSENSUAL INTIMATE IMAGERY

A. Historical Context: The Proliferation of Non Consensual Pornography

Deepfakes have primarily targeted women, despite the fact that they pose a threat to both society and personal privacy. The first significant abuse of this technology was recorded in 2017, in circumstances where an anonymous Reddit account holder going by the handle posted sexual

[21] *Id.* at ¶ 43.
[22] *Id.* at ¶ 44.
[23] Aishwarya Rai Bachchan v. Aishwaryaworld.com, 2025 SCC OnLine Del 5943.
[24] *Id.* at ¶ 44.
[25] *Id.* at ¶ 38.
[26] *Id.* at ¶ 39.
[27] Silberling, Amanda, *The Taylor Swift Deepfake Debacle Was Frustratingly Preventable, Tech Crunch* (Nov. 10, 2025, 10:32 PM), https://techcrunch.com/2024/01/30/the taylor swift deepfake debacle was frustratingly preventable/.
[28] U.S. DEP'T OF HOMELAND SEC., The Increasing Threats of DeepFake Identities 5 (Nov. 15 2025), https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

 [ISSN 2581-5369]

movies featuring the faces of female celebrities artificially superimposed. Similar deepfake movies have since become widely circulated, severely violating women's privacy and dignity.[29]

The first significant criminal use of this technology is non consensual pornography, which makes up about 96% of all deepfakes on the internet. Sexual content keeps spreading on platforms like Facebook and other social network sites like Instagram, and WhatsApp, and many instances go unsolved because it is impossible to identify the offenders[30].

The majority of online harm and deepfake abuse targets women and LGBTQ+ individuals, research shows that sexual deepfakes take into consideration most cases, with women being the primary victims[31].

B. The Damage to Mind and Name

India symbolically respects women via religious devotion, festivals, and events like International Women's Day, but the actual lives of women in the country frequently present a completely different picture.[32] Despite constitutional guarantees of equality and dignity, women are nonetheless subjected to a variety of forms of exploitation, such as new types of digital abuse made accessible by technology.[33] The quick digitization of ordinary life has affected people's perceptions of personal safety. Women are increasingly exposed to new types of cyber based victimization in the home, which was traditionally thought to be a private and protected place[34]. An atmosphere of uneasiness and psychological discomfort has been brought about by the rise in cybercrimes, which range from identity theft and privacy violations to the unapproved sharing of photographs. Among these, deepfakes are among the most harmful technical expressions of aggression against women[35]. A growing industry of deepfake creators now offers personalized videos for prices as low as $2.99, fueling a market that relies on photos ripped from the victim's own social media profiles[36].

C. Societal Dichotomies: Cultural Reverence vs. Digital Exploitation

The misuse of deepfakes can lead to considerable psychological discomfort, including embarrassment, anxiety, and trauma, damage reputations, inflict financial and professional

[29] Deeksha Kumari, *Deepfake Technology and Legal Issues*, 2 LAWFOYER INT'L J. DOCTRINAL LEGAL RSCH. 234, 245 (2024).
[30] *Id.* at 238 239.
[31] BHATTACHARJEE et al., *supra* note 5, at 1199
[32] Vishakha Tyagi, *Victimization of Women in Cybercrime: An International Perspective*, 6 INT'L J.L. MGMT. & HUMAN. 1888,1889 (2023).
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Anne Pechenik Gieseke, "*The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479,1485 (October 2020).

harm, and disproportionately expose women to sexual exploitation through deepfake sexual media produced without permission[37]. Cyberspace abuse has special characteristics that amplify harm done and make it harder to identify[38]. The misuse of deepfakes can lead to considerable psychological discomfort, including embarrassment, anxiety, and trauma, damage reputations, inflict financial and professional harm, and disproportionately expose women to sexual exploitation through non consensual deepfake pornography. As a result of globalization of digital technologies, dangerous content may be produced anonymously and spread quickly via the internet, reaching people all over the world. More than half of victims are unaware of the identity of their attacker, which exacerbates their feelings of helplessness, anxiety, and misery[39]. Women faced more than twice the risk compared to men to encounter severe types of abuse (such as doxing, revenge porn, and threats of bodily harm) and are threefold more likely to encounter different forms of abuse online (such as online harassment, threats, sexualization, and stalking)[40]. Even though the majority of individuals who are affected by nonconsensual deepfake pornography do not now have access to significant remedies, sexual privacy deserves the highest level of protection[41].

IV. SYNTHETIC DISINFORMATION, MEDIA INTEGRITY, AND SYSTEMIC LEGAL GAPS

Fake news refers to deceptive content aimed at influencing public sentiment for political or economic benefit [42]. AI generated false news and material, particularly deepfakes, undermines democracy, national security, and public confidence by deceiving people, supporting illegal or violent activity[43]. The false film of President Zelensky of Ukraine during the Russia Ukraine war demonstrated how deepfakes have the potential to generation and spread of misleading information and deceive the public[44]. Deepfakes have grown significantly in recent years. Disinformation is made more convincing and vivid by deepfakes. Even when they are exposed as fraudulent, they have the power to stoke public opinion or support conspiracies. The visual realism of AI generated videos, such as fictitious political remarks or sex scenes, can cause indignation, embarrassment, or discord. News companies may broadcast bogus videos that appear authentic in an effort to be first, deepfakes dramatically harm journalism by misleading

[37] BHATTACHARJEE et al., *supra* note 5, at 1200.
[38] Jennifer Laffier & Aalyia Rehman, *Deepfakes and Harm to Women*, 3 J. DIGIT. LIFE & LEARNING 1, 5 (2023).
[39] *Id.*
[40] *Id.*
[41] GIESEKE, *supra* note 38, at 1481.
[42] Christopher Whyte, *Deepfake News: AI Enabled Disinformation as a Multi Level Public Policy Challenge*, 5 J. CYBER POL'Y 199,200 (2020).
[43] *Id.* at 204.
[44] Maria Paz Sandoval , Maria de Almeida Vau, John Solaas & Luano Rodrigues, *Threat of Deepfake to the Criminal Justice System: A Systematic Review*, 13 CRIME SCI. 1,2 (2024).

 [ISSN 2581-5369]

the audience and destroying their reputation[45].

A. Case Study: Media Impersonation and Intermediary Liability

In T.V. Today Network Limited v. Google LLC[46], the Delhi High Court dealt with a phony YouTube channel that used deepfake impersonations and fake videos to mimic journalist Anjana Om Kashyap. The court observed that these channels result in significant harm and the spread of false information. It concluded that the journalist's personality rights are violated by this unlawful commercial exploitation. Consequently, the Court issued an ad interim injunction mandating that Google remove the phony channel within 48 hours.

B. Institutional Responses to Misinformation

The Court ruled in Gaurav Bhatia v. Naveen Kumar[47] that AI generated deepfake movies disseminating misleading information inflict irreversible reputational damage. The Court mandated their removal, emphasizing that fake or deceptive digital content cannot be protected by the right to free speech. The Reserve Bank effectively countered fake news and deepfake videos during the year through timely clarifications, press releases, and public awareness campaigns to maintain trust and financial stability[48].

V. DEEPFAKE PORNOGRAPHY

The topic of deepfake porn originally came to light in 2017 when the American media was enamored with the high-profile case of Gal Gadot's face being superimposed on a porn actress' body image[49]. Both sexually explicit deepfakes and revenge porn involve the release of private content without consent and cause severe, long-lasting emotional, psychological, and social trauma to victims.[50]

A. The gaps in real protection

The sole victims of nonconsensual deepfake pornography are women.[51] Sources claim that between December 2018 and September 2019, the creation and dissemination of deepfake videos rose by roughly 100%. Nearly 96% of these films on deepfake pornography websites are

[45] Al Amin Hossain, *Addressing Deepfake through the Existing Legal Strategies in Bangladesh: An Assessment*, 7 INT'L J. L. MGMT. & HUMAN. 2260,2264 (2024).
[46] T.V. Today Network Limited v. Google LLC, 2025 SCC OnLine Del 4587
[47] Gaurav Bhatia v. Naveen Kumar, MANU/DE/2837/2024
[48] Reserve Bank of India, Annual Report 2024 25 at 206 (2025).
[49] Karolina Mania, *Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study*, 25 TRAUMA, VIOLENCE & ABUSE 117, 117 (2024).
[50] Andrea Rizzica, *Sexually Explicit Deepfakes: To What Extent Do Legal Responses Protect the Depicted Persons?* 14 (Apr. 29, 2021) (unpublished Master's thesis, Tilburg University).
[51] GIESEKE, *supra* note 38, at 1482.

 [ISSN 2581-5369]

sexual in nature, and all of them comprise women as victims.[52] Since sexual privacy is at the highest level of privacy values, it requires both recognition and defense measures, just like all other recognized privacy violations. There is currently no appropriate legal remedy that directly provides compensation to the majority of victims of nonconsensual deepfake pornography.[53] To prevent psychological and reputational injury, non consensual deepfake pornography has grown to act as a significant legal problem, leading to laws like Australia's Criminal Code Amendment (Deepfake Sexual Material) Act[54].

With over 5000 websites spreading non-consensual sexual content, deepfake content authors having accessibility to utilize fourty two open-source machine learning tools, and sizable online groups with a membership exceeding 500,000, the growing extent of harm shows the inadequacy of current legal remedies for victims[55].

VI. INTELLECTUAL PROPERTY CHALLENGES AND COPYRIGHT VIOLATIONS

Using a copyrighted work to create a deepfake without permission may be regarded as copyright infringement unless the use is protected by an exception or limitation[56]. Unauthorized adaptations or changes of original works are prohibited by copyright law, and deepfakes by their very nature entail the unapproved manipulation of audio, video, or image[57]. The most common cause of copyright issues with deepfakes is the superimposition or switching of voices or likenesses in copyrighted images, videos, or songs[58]. The original creator's exclusive economic rights are violated when deepfake videos are designed for commercial gain since the fake creator makes money while the real author receives nothing[59].

A. Economic Rights and Statutory Remedies under the Copyright Act

The phrase cinematograph film means any visual recording, including the audio recording associated therewith; it also refers to any work brought into existence using a method similar to cinematography, such as video films[60]. As a rule, the creator is the primary rights holder in relation to the copyright; nevertheless, if a photograph or cinematographic film is created for a

[52] *Id.*
[53] *Id.*
[54] Tania Kukreja, *Deepfakes as a Tool for Criminal Activity*, 5.4 JCLJ 224, 239 (2025).
[55] Ngonidzaishe T. Gotora, *Unmasking Deception: Deepfake Regulation in the Context of South African Law, Could a Rethinking of Performers' Protection Rights Be the Answer ?*, 32 INT'L J. L. & INFO. TECH. eaae026, at 6 (2024).
[56] Kyungsuk Kim, *Deepfakes: Challenges to Intellectual Property Rights in South Korea*, 74 GRUR INT'L 532, 535 (2025).
[57] *Id.*
[58] *Id.*
[59] Shriya Sayanak, *A Study on Deepfakes and Copyright Infringement*, 6 INT'L J.L. MGMT. & HUMAN. 3541,3545 (2023).
[60] Copyright Act, 1957, § 2(f), No. 14, Acts of Parliament, 1957 (India).

monetary consideration, the author's employer is the first owner[61]. With respect to a photograph, the photographer, is the author[62]and as far as a sound recording or cinematograph film is concerned, the producer is the author[63].

The the intellectual property rights holder in a motion picture or audio recording has the singular right to make another sound recording with the same sounds or to grant permission for the film's reproduction, including still images from any portion of it[64]. Also the copyright holder possesses the principal right to allow or engage in the work's storage in all form, to sell, lease, or or put up for sale or or execute any replicas of it provided for rent, together with circulate the content to the general public[65].

What constitutes copyright infringement is precisely described by the Act. Therefore, any individual or group that uses someone else's images, videos, or audio recordings to generate or distribute deepfakes online without that person's consent may be held accountable for violating that person's copyright[66].

When a work's copyright is violated, the copyright holder has the right to civil remedies such damages, an account of profits, and injunctions[67]. However, the remedy is restricted to an injunction and recovery of profits made from the infringement, as rules by the court, if the infringer demonstrates that they lacked awareness that copyright existed in the work[68].

B. Moral Rights, Integrity, and the Fair Dealing Defense

In the case before the Delhi High Court, Amar Nath Sehgal v. Union of India[69] clarified it's position that author retains the entitlement to preserve, defend, and nurture his creativity. An author holds the library to forbid, or initiate a demand for damages resulting from every twisting, defacement, restructuring or other act carried out on their work[70].

If a deepfake video is created for research, education, criticism, news reporting, or parody, it may occasionally be protected under fair use[71]. This applies only when the video adds new meaning or commentary without harming the original creator's rights or profits. But if the

[61] *Id.* § 17.
[62] *Id.* § 2(d)(iv).
[63] *Id.* § 2(d)(v).
[64] *Id.* § 14(d),(e).
[65] *Id.*
[66] *Id.* § 51
[67] *Id.* § 55
[68] *Id.*
[69] Amar Nath Sehgal v. Union of India, 2005 SCC OnLine Del 209 : ILR (2005) 1 Del 236 : (2005) 117 DLT 717 : (2005) 30 PTC 253 : (2005) 2 CCC 194 : (2005) 1 RAJ 441
[70] Copyright Act, 1957, § 57, No. 14, Acts of Parliament, 1957 (India).
[71] *Id.* § 52.

 [ISSN 2581-5369]

deepfake misleads people, damages someone's reputation, or is used for commercial gain, it won't be protected under fair use.

VII. POLITICAL IMPLICATIONS AND THE EXISTING STATUTORY REGIME

India was ideal for localized manipulation because of its linguistic diversity[72]. In regional accents that suggested intimacy and assurance, translated comments and fictitious endorsements emerged[73]. Messaging apps propagate deepfakes faster since private groups hide them from fact checkers, and local language, images, and lip sync make them look real especially on low-quality phones making identification and correction tougher, as shown during India's 2024 elections[74].

India's democratic integrity is seriously threatened by the emergence of deepfake technology, since AI generated fake audio and video content could be used as a weapon to disseminate false information and sway voters' opinions during elections[75]. Deepfakes are being used in India's electoral process to influence young voters through WhatsApp based scratch groups, delivering targeted political misinformation[76]. India's electorate, approximately 900 million eligible voters and poor levels of digital literacy, is especially susceptible to AI generated deepfakes that magnify misinformation that has already influenced previous elections by making bogus narratives appear real[77]. Deepfake technology might enable widespread disinformation campaigns, where AI-generated texts and videos that provocative or wrongly portray opposition leaders could worsen divide and possibly spark societal unrest.

AI-powered propaganda and microtargeted disinformation can subtly influence voter behavior, decrease trust in institutions, raise polarization, fuel political violence, and disrupt electoral processes by sending out convincing deepfakes and misleading content that confuses the public and negatively impacts democratic participation[78].

A. Comparative Analysis of Political Deepfakes

In the foregoing years, the invention required to develop deepfakes has matured into more widely available and inexpensive, and their quality has greatly improved[79]. Political deepfakes

[72] Mst Rafia Islam & Azmine Toushik Wasi, *Deepfakes in Political Manipulation: Evaluating Risks Under the AI Act* (2025), https://openreview.net/forum?id=Kt9bSLxDih.
[73] *Id.*
[74] *Id.*
[75] GEORGE, *supra* note 7, at 76.
[76] Vaishnavi Kulkarni & Bhanusshre Sivaramachandran, *Tackling the Multifaceted Legal Dilemmas of Deep Fake Technology*, 4 JUS CORPUS L.J. 217,220 (March May 2024).
[77] *Id.*
[78] Masabah Bint E. Islam et al., *AI Threats to Politics, Elections, and Democracy: A Blockchain Based Deepfake Authenticity Verification Framework*, 2 BLOCKCHAINS 458,467 (2024).
[79] Lindsey Joost, *The Place for Illusions: Deepfake Technology and the Challenges of Regulating Unreality*, 33 U.

have the power to affect how the public thinks leaders by making fake content appear credible and emotionally relevant. Two cases of how manipulated videos have been used globally to damage reputations and influence elections are the widely shared 2019 video that showed U.S. Speaker Nancy Pelosi slurring her speech and the UK's Future Advocacy project, which produced synthetic media involving Boris Johnson and Jeremy Corbyn to highlight election fraud tactics[80]. AI generated deepfakes were first used in politics in India in 2020 when recordings related to politician Manoj Tiwari slamming political opponent Arvind Kejriwal in both Haryanvi and English became viral in WhatsApp groups prior to the Delhi elections[81].

AI has the ability to automatically create and disseminate fake information, social media posts, and other deceptive content, frequently with the intention of manipulating particular voter demographics with targeted misinformation[82]. Such AI driven efforts used social media algorithms to increase reach and significantly affect voter views during the 2020 U.S. presidential election by disseminating false information about candidates and voting procedures[83]. Anyone accused of wrongdoing could claim a video is fake, actual evidence may begin to be questioned. This gradually undermines our confidence in any audio or video we come across online, making it more difficult to determine the truth.

VIII. STATUTORY FRAMEWORKS AND ENFORCEMENT MECHANISMS

An examination of 96 recent bills reveals that although politicians are focusing more on the negative effects of deepfakes, particularly when it comes to children, the rules are still dispersed and ambiguous, lagging behind the speed of technology and necessitating a more robust, cohesive framework[84].

India presently lacks a specific statute governing deepfakes; however, applicable legal provisions exist, including the Information Technology Act[85] and the Bharatiya Nyaya Sanhita[86], and also particular legislations like the Indecent Representation of Women Act[87], the Representation of the People Act[88] concerning election related deepfakes, and the Digital Personal Data Protection Act[89] addressing privacy infringements. Deepfake misuse falls under

FLA. J.L. & PUB. POL'Y 309,314 (Spring 2023).

[80] Shinu Vig, *Regulating Deepfakes: An Indian perspective*, 17 J. STRATEGIC SEC. 70, 74 (2024), https://doi.org/10.5038/1944 0472.17.3.2245.

[81] *Id.*

[82] ISLAM et al., *supra* note 80, at 466.

[83] *Id.*

[84] CHEN., *supra* note 11, at 18.

[85] Information Technology Act, No. 21 of 2000, India Code (India).

[86] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (India).

[87] Indecent Representation of Women (Prohibition) Act, No. 60 of 1986, India Code (India).

[88] Representation of the People Act, No. 43 of 1951, India Code (India).

[89] Digital Personal Data Protection Act, No. 22 of 2023, India Code (India).

 [ISSN 2581-5369]

cybercrimes which includes identity theft, posting pornographic or altered content online, publishing or transmitting obscene material are covered by the IT Act[90]. When deepfakes result in criminal harm, such as impersonation, fraud, threats, or inciting violence, the Bharatiya Nyaya Sanhita is applicable. Other laws, such as the Representation of the People Act for election related disinformation, the Indecent Representation of Women Act for sexually manipulated media, and the Digital Personal Data Protection Act for unauthorized use of someone's voice, image, or biometric data, take over for specific infractions.

A. Constitutional Mandates: The Right to Privacy and Puttaswamy

The Supreme Court's monumental verdict of 2017 in Justice K.S. Puttaswamy (Retd.) v. Union of India[91] serves as the basis for the legal fight against deepfakes in India. A nine judge panel pronounced that the right to privacy acts as a constitutional privilege ensured under Article 21 of the Constitution[92]. Because it establishes control over one's own body and image, this decision is crucial. To put it simply, it is unlawful to utilize someone's voice, images, or videos to produce deepfakes without that person's consent since it encroaches on their fundamental right to privacy and control over their personal information.

B. Information Technology Act

i. Section 66D

In this section anti catfishing and anti fraud regulations are provided. It declares that it is a major offence to use a computer or communication equipment to masquerade as someone else in order to cheat. Despite being drafted before to the AI boom, this rule clearly addresses contemporary risks such as Deepfakes. You are breaching the law if you use AI to swap looks or mimic voices in order to deceive someone or perpetrate fraud. If found guilty, the punishment is severe, with a utmost custodial term of three years in prison and a monetary penalty of up to ₹1 lakh[93].

ii. Section 67

Sharing offensive or sexually explicit deepfake movies online is illegal under this section, if caught, the punishment is detention for a term of up to five years and a cash penalty of up to ten lakh rupees[94].

[90] Information Technology Act, No. 21 of 2000, §§ 66C–66E, 67–67B, India Code (India).
[91] Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC (SUPP) 1841 : AIRONLINE 2018 SC 237
[92] INDIA CONST. (1950).
[93] Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).
[94] *Id*. § 67.

 [ISSN 2581-5369]

iii. Section 69A

The government can effectively restrict internet content by using Section 69A. If deepfakes endanger the nation's security, independence, or public tranquility, it permits authorities to order their removal[95].

iv. Section 72:

Confidentiality violations are penalized under Section 72. Anyone who disseminates deepfakes that violate someone's privacy faces a custodial sentence of up to two years and a fine[96].

C. Bharatiya Nyaya Sanhita

i. Section 356

It is illegal to harm someone's reputation under Section 356. A person may face a two year prison sentence, a fine, or a community service requirement if they disseminate deepfakes or fake news to disparage others[97].

ii. Section 294

One important clause that prohibits digital obscenity is Section 294 of the BNS. It makes it illegal to sell, distribute, or exhibit pornographic content in public, including electronic form. Accordingly, the first offense of sharing sexually explicit deepfakes carries a maximum sentence of two years in prison[98].

iii. Section 75

Deepfake pornography is considered a serious form of sexual harassment under Section 75 of the BNS. Making sexually colored remarks or showing pornography against the will of a woman are particularly prohibited by law. Criminals who produce or distribute such content if done with the intent to harass women, may attract imprisonment of up to three years[99].

iv. Section 78

Monitoring a woman's online activities is considered stalking under Section 78 of the BNS, which makes it illegal to follow a victim online in order to gather images for deepfakes. This offense has a outmost jail term of three years and a financial sanction for a first conviction; however, the penalty rises to five years in prison and a fine for a second or subsequent

[95] *Id*. § 69A.
[96] *Id*. § 62.
[97] Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).
[98] *Id*. § 294.
[99] *Id.* § 75.

 [ISSN 2581-5369]

conviction[100].

v. Section 318

The main clause for deepfake financial frauds is Section 318(4) of the BNS, which deals with the crime of cheating when the perpetrator dishonestly induces the person deceived to deliver any property. Therefore, an offender faces up to seven years in prison and a fine if they utilize distorted media to trick a victim into transferring money or assets[101].

vi. Section 319

Because deepfakes basically require pretending to be someone else, Section 319(2) treats them as cheating by personation, a transgression subject to penalty as much as five years in penal institution even if the deceit does not immediately result in financial loss[102].

D. Indian Copyright Act

Making or sharing a deepfake that uses someone else's voice, image, or video without that person's permission may be seen as copyright infringement since it involves the unlawful use of protected material. Section 51, which prohibits exploiting someone's exclusive property rights, may impose fines for such misuse[103].

IX. THE REGULATORY CHALLENGE OF DEEPFAKES

Governments are finding it difficult to address the issues associated with producing and disseminating synthetic media as deepfakes get more sophisticated. Even though there currently exist some some regulations that address topics like misinformation, intellectual property, and online criminality, they are insufficiently detailed to address the actual difficulties that deepfakes present[104]. They are somewhat beneficial, however there are still significant holes that must be filled.

The majority of Indian police and cybercrime units lack the sophisticated equipment and training necessary to identify deepfakes, which delays investigations and makes it difficult to prosecute perpetrators[105].The true issue is that there are no laws in India that particularly address deepfakes, and because cybercrime is cross border, it is challenging to police them because

[100] *Id*. § 78.
[101] *Id*. § 318.
[102] *Id*. § 319.
[103] Copyright Act, 1957, § 51, No. 14, Acts of Parliament, 1957 (India).
[104] Afshari, N. & Mohammadi, *The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media*. LEGAL STUDIES IN DIGITAL AGE, 2(2), 13,19 (2023).
[105] KUKREJA, *supra* note 56, at 232.

technology develops more rapidly than the legal system[106].

Since there isn't currently a distinct international cybercrime legislation, we are still developing worldwide regulations for this problem, but conventions like Istanbul and Budapest approach it as a type of online violence[107].

X. STRATEGIES TO COMBAT DEEPFAKES

The fundamental problem is that depending just on audience empowerment or detection technology will not halt AI powered misinformation since deepfake producers are always changing to evade detection, and audience empowerment calls for reliable gatekeepers that the public does not want or trust[108]. India needs to include these detection technologies into digital platforms and law enforcement so that authorities can rapidly check content and shield citizens from abuse and false information[109]. Deepfake evidence must be identified and countered by legal specialists, and institutional safeguards must be put in place to stop its abuse in the legal system[110]. To stop abuse and safeguard its citizens, India needs robust AI regulation and detection technologies, mandated watermarking, quicker removal guidelines, stringent platform accountability, public awareness, international collaboration, and an ethics framework[111]. Training law enforcement, educating the public through digital literacy, and investing in advanced research to improve deepfake detection are critical to remain ahead of this quickly growing threat[112].

So as to effectively address the growing threat of deepfakes, appropriate laws that directly deal with this problem is required. The Information Technology Act refuses to sufficiently deal with the issue. Either a new legislation India must implement rules specifically targeting deepfakes, or the current Act has to be amended to clearly clarify offenses and penalties.

XI. SUGGESTED AMENDMENTS AND REGULATORY REQUIREMENTS

Similar to the Malicious Deep Fake Prohibition Act[113] in the US, India needs a precise legal definition of deepfakes that characterizes them as digitally produced content that appears

[106] Adyasha Behera & Bhanu Pratap Singh, *Deceptive Realities: India's Legal and Ethical Framework against Digital Forgeries and Deepfake Crimes*, 7 INT'L.J. MGMT. & HUMAN. 2211,2213 (2024).
[107] BHATTACHARJEE et al., *supra* note 5, at 1202.
[108] WHYTE, *supra* note 44, at 211.
[109] BEHERA et al., *supra* note 108, at 2219.
[110] Molly Mullen, A New Reality: Deepfake Technology and the World around Us, 48 MITCHELL HAMLINE L. REV. 210,224 (2022).
[111] Nikita Agarwal, *Legal Challenges of Deepfake Technology and AI Generated Content in India, Jus Corpus* (Apr. 21, 2025), https://www.juscorpus.com/legal challenges of deepfake technology and ai generated content in india/.
[112] SANDOVAL et al., *supra* note 46, at 10.
[113] Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Cong. § 2 (2018).

authentic enough to deceive a reasonable viewer. By establishing this benchmark, damaging deceit can be distinguished from innocuous parody.

Stronger forensic technology and expert involvement in evidence verification are desperately needed. In a UK custody case, a mother presented threatening audio against her husband, but he demonstrated through metadata analysis that the recording was a deepfake created by software, highlighting how easily false evidence can enter courtrooms[114].

To address deepfake abuse, India requires more robust international and cross border measures. In order to establish standard regulations and facilitate cross border enforcement, a global convention on AI generated content is required. Until then, India should apply its laws extraterritorially and establish bilateral agreements to prosecute offenders overseas, supported by wider international collaboration[115].

XII. CONCLUSION

Deepfakes have significantly altered the environment of evidence, privacy, and truth. What started out as a technological advancement has been turned into a weapon, endangering India's democratic process and disproportionately targeting women with sexualized abuse. Our present inquiry reveals a terrible reality, even if Indian laws like the IT Act and the BNS provide a basic defense against the sophisticated cheap fakes and AI generated forgeries that are growing on the internet.

Our current legal system is disjointed and inadequate, which makes it much too simple for criminals to get away with deepfake abuse. We cannot continue to rely on band aid solutions or try to impose outdated legislation to address a whole new issue. If we're serious about defending the right to privacy established in the Puttaswamy ruling, then India needs a clear, a law enacted to cover how deepfakes are generated and circulated. That is the only way to bridge the gaps and keep people safe. For the legislation to genuinely work, it needs robust support structures behind it. Including provisions such as required watermarks on AI generated content, true accountability from social media platforms, and competent forensic experts who can distinguish what's real and what's faked. In essence, we are in a race against technology, which is becoming more adept at simulating reality every day. If our legal instruments don't keep up, we risk losing our capacity to believe what we see and hear. It is no longer optional to develop systems that

[114] KUMARI, *supra* note 31 at 248.
[115] Yash Bajpai, *Me, Myself and AI: Chasing Deepfakes Across Borders Without Losing Your Rights*, SCC ONLINE BLOG (Nov. 8, 2025), https://www.scconline.com/blog/post/2025/11/08/deepfake regulation rights/.

are as sophisticated as the technologies they regulate. It's important if we want truth to survive in the digital age.

*****

 [ISSN 2581-5369]