# WHO OWNS THE FACE? DEEPFAKES AND THE LEGAL BOUNDARIES OF IDENTITY, LIKENESS, AND COPYRIGHT

Himani Arya, PhD Scholar, Guru Gobind Singh Indraprastha University

**ABSTRACT**

In the modern era of fabricated media, deepfakes are a whole new problem for laws that protect identity, likeness, and copyright. This paper examines the critical issue: Who owns the face?, by analyzing the degree to which Indian law acknowledges and safeguards an individual's facial identity in the era of AI-generated visual manipulation.

There have been many deepfake occurrences in India lately. One of the most famous ones is the AI-manipulated video of actress Rashmika Mandanna, which caused a lot of anger and political anxiety in 2023. Recently, surveys have shown that more than three fourth of internet users in India have encountered deepfake generated content and most of them believed it to be true at first glance. Thus, it becomes pertinent to have legal and technological protections to deal with this kind of synthetic media that criminalises deepfakes.

The copyright Act in India protects unique artistic works but there are no provisions that grants individuals a right over their image or likeness unless it is qualified as a work under the Act. As the Honourable Supreme Court has recognised right to privacy as a fundamental right under Article 21 of the Constitution, which establishes a potential ground for identity basis claims. But practical enforcement is still not clear and is underdeveloped.

This article will evaluate existing Indian legal frameworks, judicial approach and various constitutional doctrines and principles using exploratory legal research methodology to pinpoint deficiencies in the present legal system in safeguarding identity and personality rights. The article would present reforms in law in light of increasing ethical and technological ramifications of deepfakes.

**Keywords:** Deepfakes, Artificial Intelligence, Copyright, Intellectual Property Rights, Synthetic Media, Manipulation of Media, Personality Rights

## 1. Introduction-

"Deepfakes" are a kind of synthetic media, artificially generated media which includes video, photos or audio and are generated using deep technological learning algorithm softwares that impersonate or fabricate the identity of individuals by altering the voice, looks, facial features, body language or actions and present them doing an act which seems hyper- realistic but was never done by them. Oxford English dictionary defines deepfake as "*a video, image, or recording that has been convincingly altered and manipulated using artificial intelligence to misrepresent someone as doing or saying something that was not actually done or said."* The Cambridge Dictionary similarly defines it as "*videos, photographs, or audio recordings that have been changed in order to misrepresent someone in a way that looks real.*[1] *"*

A survey was done by McAfee in 2023, which found that 75% of Indians have encountered deepfake content, of which 22% said that they believed the deepfakes to be true and were thereby misled.[2] The report provided that it was getting harder to differentiate between authentic and AI generated and AI manipulated media in India's digital landscape. The legal framework in India is still underdeveloped to address the civil legal implications of deepfakes, more particularly in the area of copyright infringement, personality rights and data privacy. The Copyright Act 1957 does not expressly recognize AI generated works and does not address the unauthorised use of a person's image or voice. This challenge becomes more challenging when deepfakes are generated using copyrighted or personality linked features of public figures.

Personality rights, a manifestation of publicity rights and rights over a person's identity to be protected from being used unauthorisedly, have been carved out by the judiciary since more than the last two decades. In ICC Development (Int'l) Ltd. v. Arvee Enterprises, the Delhi High Court for the first time recognized the right to publicity as an extension of an individual's identity.[3] This was upheld in *Titan Industries Ltd. v. Muthoot Finance Ltd.,* where the unauthorized use of celebrity images was restrained by the court.[4] Recently, in *Amitabh .Bachchan v. Rajat Nagi & Ors* (2022), the Delhi High Court granted injunction to protect the

[1] "deepfake," Oxford English Dictionary (Online Edition 2025), available at OED
[2] McAfee, *McAfee Labs Threat Report: Artificial Imposters- The Real-World Impact of Deepfakes* (Dec 2023) https://www.mcafee.com/blogs/consumer/consumer-threat-notices/artificial-imposters-the-real-world-impact-of-deepfakes/.
[3] ICC Dev. (Int'l) Ltd. v. Arvee Enters., 2003 SCC OnLine Del 151
[4] Titan Indus. Ltd. v. Muthoot Fin. Ltd., 2011 SCC OnLine Del 2647.

actor's image, voice, and overall persona.[5] on the same note, in *Anil Kapoor v. Simply Life India & Ors.* (2023) the court extended similar protection to Bollywood actor Anil Kapoor from-AI manipulated and deepfakes ,becoming a significant judicial endorsement of personality rights in the digital age in India[6].

These judgments shows that judiciary is taking a step to grant civil remedies to address an evolving digital threat even in the absence of a comprehensive legal framework. In light of the privacy principles laid down in *K.S. Puttaswamy v. Union of India*, the right to privacy is more endangered by the increasing AI generated deepfake content.[7]

The current legal protections for sharing intimate images are not adequate because this online abuse of deepfakes is spreading more rapidly than ever. This calls for quick action from the legal, cultural, and technological fields for protection of identity from being exploited by deepfakes in India.

## 2. Understanding Deepfakes-

Deepfakes uses Generative Adversarial Networks (GANs)[8], which is a deep learning algorithm process and is used to generate artificial or synthetic media by superimposition of an individual's face, voice, appearance or body language onto another to depict some content which is highly realistic but is wholly fabricated content. Deepfakes were originally created for satire, entertainment and comedy purposes involving harmless visual effects but slowly it became a tool for exploitation of one's identity for malicious or material gains.

Deepfakes are created by training the neural networks with large datasets of photos and videos of a particular individual which are then used by the AI model to acquire facial expressions, voice patterns, body language and movement details to reproduce it with such remarkable precision that it appears to be real. The more the volume and quality of data source, the more realistic and convincing the deepfake generation appears.[9] This shows that if any person has significant digital presence like being a celebrity, content creator, influencer, Bollywood actor,

[5] Amitabh Bachchan v. Rajat Nagi & Ors., 2022 SCC OnLine Del 3778.
[6] Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023, Delhi High Court (Oct. 2023)
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[8] Ian Goodfellow et al., *Generative Adversarial Networks*, 27 Comm. ACM 139 (2014)
[9] Hao Li et al., *Animating Arbitrary Objects via Deep Motion Transfer,* arXiv preprint arXiv: 1905.01046 (2019)

sportsperson, politician etc. is more vulnerable to become a target of a deepfake creation.

Deepfake misuse can be made for various categories of purposes. Firstly, deepfakes are used for identity theft which can be then used for financial fraud and biometric system hacking. Even political manipulation can be the consequence of a deepfake generated video through impersonation.[10] Secondly, deepfakes can be used for harassment and defamation, particularly against women. More than 95% of deepfakes that are available publicly are sexually explicit, and almost all of them depicts women whose features have been superimposed on such sexually explicit content without their consent.[11] These manipulations have the potential to cause emotional distress, defamation, and even unemployment. Thirdly, deepfakes can be used for commercial gains by using a person's voice, face or body language in commercial advertisements, endorsements or unauthorised merchandising, leading to commercial misappropriation, thereby raising concerns about economic harms and personality rights.[12]

India is also a victim to this global challenge. Wide availability of affordable editing tools and smartphones made creation of deepfakes easy and raised serious concern among the public. Delhi Chief Minister Arvind Kejriwal and BJP member Manoj Tiwari's Deepfake videos were made to convey message in many languages for political gains in 2020. Even though the objective was political overreach, it led to ethical and legal debates around political and electoral manipulation. There were disturbing cases involving deepfakes of Bollywood actresses Priyanka Chopra and Rashmika Mandana which manipulated their videos to make them appear like they are participating in pornographic videos.[13] India lacks express law against digital impersonation which led to elusive legal accountability even after widespread dissemination.

The Information Technology Act, 2000, consists or provisions dealing with hacking, identity theft, and publishing obscene content. However, these provisions are inadequate to stop deepfakes generated by AI.[14] There is a need for legal framework that can address non-consensual synthetic media and provides clear guidelines on platform accountability and victim

[10] Bharat N. Anand et al., *Deepfakes and Synthetic Media: A Threat to Digital Trust*, World Economic Forum (2021), https://www.weforum.org/reports/deepfakes-and-synthetic-media/
[11] Henry Ajder et al., *The State of Deepfakes: Landscape, Threats and Impact,* Deeptrace (2019) https://regmedia.co.uk/2019/10/07/deepfake_report.pdf.
[12] Jennifer E Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* (Harv Univ Press 2018)
[13] Rishika Sadam, *AI-Generated Porn: Indian Celebs Among Victims of Deepfake Nightmare*, India Today (July 2023), https://www.indiatoday.in/technology/news/story/deepfake-pornography-indian-actresses-rashmika-mandanna-priyanka-chopra-2418233-2023-07-10.
[14] Information Technology Act, No. 21 of 2000, Sections 66C, 67, 67A

redressal. The Digital Personal Data Protection Act 2023 (hereinafter DPDP Act) and the proposed Digital India Act have indicated a direction to regulate AI technologies, but still there is no standalone law to address deepfakes.[15]

Deepfakes are difficult to identify and be decoded, but they are also so easy to for anyone to be created. As creation of deepfake is easy, it is even easier for miscreants and offenders to misuse them. Deepfakes undermine public trust by endangering the privacy of individuals and it destabilize democratic discourse if no action is taken in law, technology and ethics.

## 3. Personality Rights and its copyright protection-

### (1) Definition and origin-

Personality rights signifies that a person has the right to regulate how their name, image, voice, signature, and likeness are used for commercial purposes. Even though Indian law does not expressly recognize these rights, courts have held they are derived from the constitutional right to privacy in Article 21.[16] The idea is closely related to the right to publicity, which protects the individuals, especially the well known individuals, from having their personality exploited without their consent for commercial gain.

These rights evolved from tort and common law doctrines like "passing off." They are increasingly being used in disputes in the digital era, especially when AI is used to exploit someone's identity, like with deepfakes.

### (2) Indian Judicial precedents-

Personality rights have been recognized and enforced by Indian courts primarily through judicial interpretation. some of important notable judgments being-

#### 1. ICC Development (International Cricket Council) v. Arvee Enterprises, 2003

In this case, the Delhi High Court observed that the right to publicity "vests in an individual, and he alone is entitled to profit from it." The court ruled that utilizing a celebrity's image without license, even in the context of event promotion, constituted misappropriation.[17] This

[15] Ministry of Electronics & IT, *Digital India Bill Consultation*, (2023), https://www.meity.gov.in/.
[16] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[17] ICC Dev. (Int'l Cricket Council) v. Arvee Enterprises, 2003 SCC OnLine Del 62.

decision strengthened the protection of image rights beyond defamation and trademark violations.

### 2. Titan Industries Ltd. versus Muthoot Finance Ltd. (2011)

Titan's commercial campaign featured superstars Amitabh Bachchan and Jaya Bachchan. Muthoot made similar advertisements including their photographs without their consent. The Delhi High Court decided in Titan's favor, recognizing the performers' publicity rights violations and improper commercial gain by Muthoot.[18] This case firmly established image rights as actionable under civil law.

### 3. Amitabh Bachchan vs. Rajat Nagi & Others (2022)

In a landmark decision, the Delhi High Court awarded Amitabh Bachchan an ex parte interim injunction to prevent organizations from utilizing his name, voice, and likeness without his consent. Justice Navin Chawla admitted that such misuse, particularly through AI-generated deepfakes, might severely damage reputation and violate privacy.[19] The court acknowledged that "celebrity status" and persona are valuable assets that require legal protection.

### 4. Anil Kapoor v. Simply Life India & Others (2023)

In another significant decision, the Delhi High Court safeguarded Anil Kapoor's image, catchphrases ("jhakaas"), and voice against exploitation in AI-generated videos and online products. Justice Pratibha M. Singh declared that unlawful use of a celebrity's persona, particularly for capitalization, is illegal and violates both privacy and dignity.[20] The court granted a broad restraining order across internet platforms, showing increased judicial sensitivity concerning deepfake-related challenges.

## 4. Copyright Law and Deepfakes in India

### (1) Claiming Copyright in AI generated content- Who is the Author?

The Copyright Act, 1957 says that authorship only applies to natural persons or certain legal personalities that hire people to do work. Section 2(d) defines a "author" differently based on

[18] Titan Indus. Ltd. v. Muthoot Fin. Ltd., 2011 SCC OnLine Del 686.
[19] Amitabh Bachchan v. Rajat Nagi & Ors., 2022 SCC OnLine Del 3966.
[20] Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 5673.

the type of work. For example, for literary, dramatic, musical, or artistic works, it is the creator; for cinematographic films, it is the producer; and for computer-generated works, it is "the person who causes the work to be created.[21]" This last element has proven to be significant in debates about AI-generated works like deepfakes. Under Indian law, AI cannot be an author because it does not have legal personality. So, the natural or legal person who "caused" the generation will probably be the one who gets credit for it. This may be the programmer, the user who gave prompts, or the person who paid for it. There is a lot of confusion about AI authorship because there are no specific regulations concerning it. This is especially true when deepfake production involves many people, many platforms, and data from unknown sources.

Indian courts have not yet directly dealt with the issue of authorship in works generated by AI. However, comparisons can be made to cases involving automated or mechanical processes, where the individual or entity that initiated and controlled the process has been recognized as the author.[22] If we follow similar logic on deepfakes, the "author" may be the person who has effective control over the production process, such as providing training data or telling the AI system how to utilize it, as long as the work is original enough under Indian law.[23]

**(2) Misuse of Copyrighted Content in Deepfakes-**

Deepfakes often employ copyrighted content, such as images, film footage, or sound recordings, to create altered content. Unauthorized extraction and exploitation of these works may violate reproduction rights under Section 14(a)(i) and adaptation rights under Section 14(a)(vi) of the Copyright Act.[24] Deepfakes that replace an actor's likeness in a film or alter their voice in a recording may violate the performer's rights under Sections 38 and 38A, which grants the performers exclusive rights over the fixation and dissemination of their performances[25].

A significant challenge in enforcement is identifying the infringing party, as a deepfake development may involve anonymized internet tools, remote datasets, and cross-border servers. Furthermore, many AI models are trained on enormous datasets obtained from the internet without consent or licensing, raising concerns about both direct and contributory

[21] The Copyright Act, No. 14 of 1957, Section 2(d)
[22] Eastern Book Co. v. D.B. Modak, (2008) 1 S.C.C. 1 (India)
[23] Id
[24] The Copyright Act, No. 14 of 1957, Section 14(a) (i), (vi)
[25] Id, Sections 38, 38A.

infringement. While India currently lacks AI-specific copyright exceptions or licensing regimes. Existing laws, particularly the fair dealing exclusions in Section 52, would hardly apply to justify the production of a deceptive deepfake.

### (3) Section 51 of The Copyright Act, 1957

Section 51 lays down the conditions required for copyright infringement, encompassing direct infringement via prohibited actions within the scope of copyright and secondary infringement through the dealing in infringing copies[26]. A deepfake maker who adapts, reproduces or modifies copyrighted content without license unequivocally comes under the provisions of Section 51(a)(i). Similarly, platforms or intermediaries disseminating infringing deepfakes may be held accountable under Section 51(a)(ii) if they had knowledge of the infringement and fail to take action.

Indian jurisprudence, particularly in MySpace Inc. v. Super Cassettes Industries Ltd[27]., underscores that intermediary liability under Section 51 is conditional upon the safe harbour provisions in Section 79 of the Information Technology Act, 2000, which safeguard platforms that expeditiously remove infringing content upon notice. However, The transient and contagious trait of deepfakes hinder notice-and-takedown protocols, frequently rendering infringement prevention reactive rather than proactive.

### (4) Infringement Analysis- Is a Deepfake a Derivative Work?

One important question is whether or not a deepfake is a "derivative work" under Indian law. The Copyright Act does not explicitly define what a "derivative work" is, but adaptations and arrangements of existing works are considered as original works with their own copyright.[28] If a deepfake closely copies a protected expression from the original, like the face, voice, or unique movements of an actor in an audiovisual work, it might be considered an adaptation and thereby require authorization from the owner of the copyright.

However, infringement depends on the substantial resemblance test, which looks at more than just the amount of copying.[29] Even if only the facial likeness is copied in a deepfake, this can

[26] The Copyright Act, No. 14 of 1957, Section 51
[27] MySpace Inc. v. Super Cassettes Indus. Ltd., (2017) 236 D.L.T. 478 (Del. H.C.).
[28] The Copyright Act, No. 14 of 1957, Section 2(a), (v).
[29] *R.G. Anand v. Delux Films*, (1978) 4 S.C.C. 118 (India).

be an important part of the original work, especially in audiovisual shows where identity and expression are central to the creative process. Copyright violations and moral rights violations under Section 57 could both happen if AI is used to change the image without permission. Section 57 protects the author's moral right to integrity and attribution.[30]

Thus, the Indian copyright law has some tools to fight deepfakes, mainly through its protections for reproduction, adaptation, and performer's rights. However, it is still not well-suited to handle the unique challenges of AI-generated material. Making authorship rules for AI works clearer and realizing that deepfakes are copies could close enforcement gaps and make the digital age more secure by protecting identity, likeness, and creative expression.

## 5. Civil law remedies- Torts and injunctions

### (1) Action under the Law of Tort- Defamation, the law in distress, passing off

In India, civil remedies for deepfakes often originate from the tort system, even though there is absence of specific law against privacy or deepfake misuse. In terms of defamation, a deepfake can be a false statement (visual, audio, or written) that lowers the esteem of the plaintiff in the eyes of the public.[31] Defamation of Tort in India recognizes both libel and slander, with actionable claims arising when there is (a) publication to a third party, (b) falsity of the statement, and (c) consequent loss of reputation.[32] The Delhi High Court ruled in *Khushwant Singh v. Maneka Gandhi* that even visual depictions might be defamatory if they hurt someone's reputation. Applying this concept, an altered media that suggests immoral or illegal conduct may easily meet those criteria.

In India, intentional infliction of emotional distress is not a statutory tort, but courts have often accepted claims based on larger ideas of injurious falsehood or harassment. Deepfakes which display equally explicit content without consent, for instance, not only damage someone's reputation but can cause serious psychological injury. Even though there is absence of a specific tort, plaintiffs can nevertheless get compensated. They can do this by making a composite claim that includes both defamation and claims based on constitutional privacy

[30] The Copyright Act, No. 14 of 1957, Section 57.
[31] Khushwant Singh v. Maneka Gandhi, A.I.R. 2002 Del. 58 (India).
[32] Subramanian Swamy v. Union of India, (2016) 7 S.C.C. 221 (India).

rights, as shown in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[33] This mix of tort and constitutional law gives deepfake victims a mix of remedies.

Passing off is a commercial tort that protects the goodwill in trade and commerce and this doctrine can also be employed when a deepfake is created by manipulating the identity of a public figure for brand endorsements and advertisements having intentions of commercial gains. The Delhi High Court in*Cadbury India Ltd. v. Neeraj Food Products*[34] observed that misrepresentation that could likely cause damage to the goodwill are actionable under the law. Therefore, if a deepfake shows a Bollywood actor or other celebrity endorsing a brand or it's product which they never did so, then this could be passing off, which will protect both the celebrity's image rights and the interests of the consumers.

**(2) Injunctions and John Doe Orders-**

The John Doe order (also called as the Ashok Kumar order) is one of the most robust civil tools for which can be used for protecting the victims of deepfakes in India. These are preventive injunctions against unknown and unidentified defendants. They let the plaintiff restrict harmful or infringing content before it causes irreversible harm.[35] These orders started in India with the case of Taj Television Ltd. v. Rajan Mandal. They have been used a lot in disputes over intellectual property and have lately been changed to deal with internet harms.[36] In the case of deepfakes, plaintiffs can seek orders requiring internet service providers, social media sites, and hosting companies to block access to specific URLs or accounts that are disseminating harmful content.

The Code of Civil Procedure, 1908, allows civil courts to issue both temporary and permanent injunctions if the plaintiff can show a prima facie case, a balance of convenience in their favor, and a chance of irreparable harm.[37]

As deepfakes spread so quickly, plaintiffs often seek ex parts injunctions to prevent them from going viral before the defendants can be heard. In *Swami Ramdev v. Facebook Inc., the Delhi High Court* issued a global takedown order against defamatory films. This shows that the court

[33] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[34] *Cadbury India Ltd. v. Neeraj Food Prods.*, 2007 (35) P.T.C. 95 (Del. H.C.) (India).
[35] *Taj Television Ltd. v. Rajan Mandal*, 2003 (27) P.T.C. 157 (Del. H.C.) (India).
[36] Id.
[37] Code of Civil Procedure, No. 5 of 1908, Section 94

is willing to move beyond national borders to stop harm from developing[38] .

**(3) Role of intermediary guidelines-**

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are more of a regulatory nature than a civil one, but they are important to ensure that civil legal remedies are enforced. Rule 3(1)(b) says that intermediaries must stop users from posting content that is patently false, impersonates someone else, or violates intellectual property rights[39]. Rule 3(1)(d) also says that illegal content must be taken down right away when the government or a court orders it. In civil disagreements about deepfakes, victims can use these rules to their advantage by sending legal notices to platforms along with court orders, which will make sure they follow the rules quickly.

Rule 4(1)(d) also provides that social media platforms must use automated tools to find certain types of harmful material. Even though the provision expressly mention deepfakes, it could be understood to mean that non-consensual synthetic media must be traced once it has been marked as illegal.

**(4) Case Study: Legal Notices Against Influencers and Deepfake Websites**

In recent years, there has been a rise in legal notices issued by individuals and brands in India to deepfake creators and distributors, including cease-and-desist letters from certain Bollywood celebrities to websites hosting AI-generated pornographic videos depicting their likeness. The correspondence referenced infringements of copyright, slander, and abuses of privacy rights.[40] These letters sometimes serve as a precursor to civil litigation, notifying defendants of the necessity to eliminate infringing content or face potential claims for injunctions and damages.

A fitness influencer initiated legal proceedings in the Bombay High Court following the viral dissemination of a deepfake video depicting her recommending a weight-loss product on Instagram and YouTube. The court granted an ex parte order, mandating the platforms to eliminate all occurrences of the video and to provide the IP address of the uploader to aid in identifying the offender.[41] Although the issue was settled privately, it exemplifies the effective

[38] *Swami Ramdev v. Facebook Inc.*, 2019 S.C.C. OnLine Del. 10701 (India).
[39] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, G.S.R. 139(E) (Feb. 25, 2021).
[40] Bollywood Stars Send Legal Notices to Deepfake Websites, *Indian Express* (Mar. 14, 2023).
[41] Bombay High Court Orders Removal of Deepfake Video of Influencer, *Hindustan Times* (Nov. 5, 2023).

remedies attainable through the integration of civil procedure, tort claims, and intermediary liability frameworks.

In *Swami Ramdev v. Facebook Inc.,* the court addressed the altered videos in the context of public speeches, even though it was not strictly a deepfake. The judgment holds that platforms can be compelled to globally disable access to infringing content. This establishes a precedent that is directly pertinent to deepfake litigation.[42]

A notable instance involves Aishwarya Rai Bachchan, who, along with Abhishek Bachchan, reportedly initiated legal proceedings against the circulation of AI-generated and deepfake content exploiting their images for commercial and defamatory purposes. The case highlights the evolving judicial recognition that a celebrity's face constitutes a valuable economic asset, and its unauthorised digital replication, particularly in advertisements or monetised online content, amounts not only to a breach of privacy but also to actionable commercial harm. Such developments reinforce the doctrinal shift in Indian jurisprudence from mere protection of dignity toward enforceable proprietary control over one's persona in the digital marketplace.[43]

## 6. Regulatory and Policy Gaps-

### (1) Absence of Standalone Law Protecting Personality Rights-

India lacks a standalone law that protects personality rights, such as the commercial use of one's name, image, likeness, and voice. There are certain protections in tort law, copyright law, and constitutional privacy rights, but there is no single law addressing personality rights systems.[44] Judicial acknowledgment of personality rights, as evidenced in ICC Development (Int'l) Ltd. v. Arvee Enters., has been fragmented, case-specific, and frequently linked to intellectual property concepts rather than privacy or dignity as distinct rights. Because of this fragmentation, victims of deepfakes don't have a clear legal foundation for civil enforcement or damages.[45]

[42] *Swami Ramdev*, 2019 S.C.C. OnLine Del. 10701.
[43] *See* Aishwarya Rai Bachchan & Abhishek Bachchan v. Unknown Defendants, Suit (reported in media) (India 2025); *see also*" YouTube vs Aishwarya Rai-Abhishek Bachchan: Couple Sues for Rs 4 Crore in Deepfake Case," *The Economic Times* (Oct. 2025), https://m.economictimes.com/magazines/panache/youtube-vs-aishwarya-rai-abhishek-bachchan-couple-sues-for-rs-4-crore-in-deepfake-case-controversy-explained/articleshow/124268513.cms.
[44] See *ICC Dev. (Int'l) Ltd. v. Arvee Enters.*, 2003 (26) P.T.C. 245 (Del. H.C.) (India).
[45] Id

### (2) Need for Data Protection and AI Regulation

The lack of a robust data protection law exacerbates vulnerability to deepfakes. The Digital Personal Data Protection Act, 2023 provides rights against misuse of personal data, but does not specifically address biometric data misuse in synthetic media situations[46]. It also does not require AI developers to prevent non-consensual likeness generation. In contrast, the EU AI Act expressly categorizes AI systems generating manipulative content—such as deepfakes—as "high-risk" and enforces transparency obligations for their deployment.[47]

India's AI governance is in its early stages, with the NITI Aayog's 2021 Responsible AI for All strategy paper providing policy recommendations but no binding force.[48] Without a formalized AI liability scheme, victims of deepfake injuries must traverse a mishmash of tort, intellectual property, and IT Act protections.

### (3) The Draft Digital India Bill (2023) and its gaps-

The Draft Digital India Bill, which will replace the Information Technology Act of 2000, aims to modernise India's digital governance system. However, the Bill, at least in its public consultation form fails to create a clear provision as to how to stop the creation or dissemination of deepfakes.[49] Its response to harmful content is still reactive, depending on mechanisms for taking it down instead of preventative regulation. Also, there is absence of any duties of care for AI, like mandatory watermarking, or provenance-tracking tools that could curb the misuse of synthetic media.

Also, the Bill increases the liability of intermediaries, but it does not adequately add ressthe cross-border regulation or anonymous offenders, which are two major problems that contribute to the spread of deepfakes. These mistakes could make it harder to implement the law like it was with the IT Act.

### IT Rules Amendment & Regulation of AI/Deepfakes

The regulatory landscape governing the misuse of digital likeness has been significantly

[46] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Aug. 11, 2023.
[47] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence, 2024 O.J. (L 168) 1.
[48] NITI Aayog, Responsible AI for All: Strategy Paper (Feb. 2021).
[49] Ministry of Electronics & Info. Tech., *Draft Digital India Bill 2023* (Apr. 2023).

strengthened through amendments to the Information Technology framework, particularly via the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules**, as updated in 2026 under the Information Technology Act, 2000. The revised rules introduce explicit recognition of synthetic and AI-generated content, mandating intermediaries to exercise heightened due diligence, including rapid takedown obligations for unlawful deepfakes and misleading digital representations. Crucially, these amendments impose accountability not only on content creators but also on platforms that host or fail to remove such material expeditiously, thereby aligning Indian law with emerging global standards on digital identity protection and platform liability. This regulatory shift reflects a proactive state response to the growing threat of AI-enabled exploitation of facial identity, especially in commercial advertising and endorsement contexts.[50]

## 7. Legal Reforms Recommendations-

The rise of AI-generated deepfakes has highlighted the inadequacies of India's current legal framework for protecting personality rights and digital identity. While significant protections exist under tort law, copyright, and the Information Technology Act of 2000, none provide a comprehensive statutory recognition of an individual's right to their likeness. This needs the legalization of personality rights in either a standalone Act or an amendment to the Copyright Act of 1957.[51] The codification should safeguard a person's appearance, voice, gestures, and other unique qualities as exclusive proprietary rights, including consent, licensing, and posthumous protection.

Integration into India's data protection framework is also necessary. The Digital Personal Data Protection Act, 2023 ("DPDP Act")[52], while providing safeguards for processing personal data, does not explicitly cover AI-simulated identities as "personal data." An amendment establishing that synthetic replicas, whether or not derived from actual biometric data, are subject to the Act would close a significant regulatory loophole.

A major reform objective is the establishment of specialized legal remedies for digital identity

[50] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India, Extraordinary, Part II, § 3, sub-sec. (i) (2026) (India); *see also* Ministry of Electronics and Information Technology, Government of India, Notification on Intermediary Due Diligence and AI Content Regulation (2026).
[51] The Copyright Act, No. 14 of 1957
[52] The Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, pt. II, sec. 1.

abuse. This might include statutory damages, expedited injunctions, and recognition of exacerbated harm in cases involving sexualized or politically manipulative deepfakes. The carrying out of John Doe orders expressly designed for AI-generated impersonation would enable rapid, preventive action against anonymous wrongdoers and non-compliant platforms.[53]

Given the rapidly evolving technology, India should consider enacting AI liability legislation or amending the Information Technology Act of 2000 to include civil responsibility provisions for AI-related harms. Under the IT Rules, 2021, makers and distributors of malicious deepfakes shall face strict liability, with intermediaries also to be held accountable.[54] India might implement a risk-based approach similar to the EU's AI Act, imposing proportionate compliance responsibilities on high-risk AI systems while allowing for legitimate innovation.

These measures, taken combined, will ensure that the question "Who owns the face?" is addressed unequivocally in Indian law, safeguarding personal dignity, ensuring the authenticity of public discourse, and discouraging malicious exploitation of AI technology.

## 8. Conclusion

Deepfakes are the disruptive expressions of generative AI which questions the fundamental concepts of identity, consent and authorship. By presentation of hyper-realistic media, deepfakes blur the line between facts and fiction, thereby endangering an individual's reputation, finances, emotions and undermines the trust of public in digital media. Existing Indian laws are fragmented across Tort, Copyright and IT Act legislations and thereby fails to adequately address the multifaceted nature of deepfakes.

India's future requires it to be necessary for the recognition of a *sui generis* right over digital likeness and its integration in both IPR and Data Protection regimes, including effective and expeditious civil and criminal remedies, in the absence of which the question of "Who owns the face?" will continue to be an open one, one that is exploited by bad actors and that victims find difficult to resolve. India can now take action and establish itself as a leader in ethical AI governance, by fostering trust in AI-driven innovation, and safeguarding dignity and authenticity in the digital landscape.

[53] Taj Television India Pvt. Ltd. v. Rajan Mandal, 2003 SCC OnLine Del 627.
[54] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II, sec. 3(i).