THE STORAGE PARADOX AND ALGORITHMIC DISGORGEMENT: NAVIGATING INTELLECTUAL PROPERTY IN AI TRAINING DATA

Isha Singh, LL.M. (Business Law), Amity Law School Lucknow, Amity University, Uttar Pradesh, Lucknow

Dr. Axita Srivastava, Assistant Professor of Law, Amity Law School Lucknow, Amity University, Uttar Pradesh, Lucknow Campus

ABSTRACT

The advent of hyper-realistic generative artificial intelligence and deepfakes has precipitated a profound legal crisis in India, destabilising established conceptions of identity, authorship, and liability. This research paper interrogates the emerging "personality rights gap," demonstrating how current statutory frameworks particularly the Information Technology Act, 2000 and ad hoc judicial injunctions are inadequate against the synthetic misappropriation of an individual's capacity for action. Employing a doctrinal critique and case-study analysis of evolving jurisprudence, including the landmark Anil Kapoor judgment, the paper highlights the erosion of intermediary safe harbour protections and the unresolved intellectual property challenges inherent in AI training data. To address these systemic inadequacies, this paper proposes a novel framework of "Deepfake Torts" under company law. Drawing upon the principle of absolute liability established in Indian environmental law (M.C. Mehta v. Union of India), the research argues for holding corporate AI developers strictly and vicariously liable for harms caused by their inherently dangerous generative models. Furthermore, the paper advocates for the statutory recognition of digital persona rights and the implementation of Algorithmic Disgorgement (model deletion) to ensure the robust protection of human identity in the digital age.

Keywords: Generative AI, Deepfakes, Personality Rights, Deepfake Torts, Algorithmic Disgorgement.

1.1 Introduction: The Ontological Crisis of Identity in the Age of Synthetic Media

The advent of hyper-realistic generative artificial intelligence (AI) has precipitated a profound legal and ontological crisis, fundamentally destabilising the established juridical conceptions of identity, authorship, and liability. This Research paper interrogates the inadequacies of the Indian legal regime in addressing the proliferation of "deepfakes", synthetic media generated by techniques such as Generative Adversarial Networks (GANs) and diffusion models, which do not merely replicate human likeness but simulate human agency with a fidelity that challenges the evidentiary basis of truth itself.

The core legal problem addressed herein is the "personality rights gap." Traditional personality rights in India, evolved through judicial precedent rather than statutory enactment, are predicated on the unauthorised commercial use of a celebrity's static image or voice. Deepfakes, however, represent a qualitative leap from static infringement; they involve the hijacking of the "performance of self." When an AI generates a video of an actor endorsing a fraudulent investment scheme, or of a politician inciting communal violence, it misappropriates not just the likeness but also the persona's capacity for action. This creates a novel category of harm that straddles copyright infringement, trademark dilution, defamation, and privacy violation, yet fits neatly into none of the existing silos of Indian jurisprudence.

Furthermore, the democratisation of deepfake technology, where open-source models allow anonymous actors to create convincing forgeries on decentralised infrastructure, has rendered traditional enforcement mechanisms obsolete. The legal subject is no longer merely a corporate entity misusing a celebrity's photo for a billboard, as seen in *Titan Industries Ltd. v. M/S Ramkumar Jewellers.*[1]but often an anonymous, cross-border actor using "dark patterns" and encrypted channels.

This research paper employs a doctrinal critique and case-study analysis to argue that the current reliance on the Information Technology (IT) Act, 2000, and ad hoc "John Doe" injunctions is insufficient. It proposes a doctrinal shift toward recognising "Deepfake Torts" under company law, holding the corporate creators of hazardous AI models strictly and vicariously liable for the harms their "products" cause. This proposal draws upon the principles of enterprise liability established in Indian environmental law (*M.C. Mehta v. Union of India*).

[1] *Titan Industries Ltd. v. M/S Ramkumar Jewellers*, (2012) 50 PTC 486 (Del).

It integrates them with the fiduciary duties of directors under the Companies Act, 2013.[2]

1.2 Indian Legal Framework: A Doctrinal Analysis of Personality Rights and AI

The protection of personality rights in India is a judicial construct derived from the synthesis of the right to privacy under Article 21 of the Constitution and the common-law tort of passing off. This section analyses how these traditional frameworks are being stretched and often broken by the realities of AI-generated content.

1.2.1 The Constitutional and Statutory Basis

The Supreme Court of India, in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, established privacy as a fundamental right, which includes the right to control the commercial use of one's identity[3]. However, the transition from a "privacy-based" right to a "property-based" publicity right remains fluid in Indian jurisprudence, creating ambiguity when applied to synthetic media.

The primary statutory instrument addressing digital harms is the **Information Technology Act, 2000**, which suffers from significant lag regarding AI technologies:

- **Section 66D (Cheating by Personation):** This section criminalises "cheating by personation by using a computer resource." While theoretically applicable to deepfakes, enforcement is hampered by the high evidentiary burden of proving fraudulent *intent* (mens rea). In the context of AI, where a deepfake might be labelled as "satire" or "parody," proving the specific intent to cheat is legally complex[4]. Furthermore, the statute was drafted to address identity theft (e.g., phishing) rather than identity *simulation*.

- **Section 66E (Violation of Privacy):** This section penalises the capture and transmission of images of "private areas" of a person without consent. This provision is severely limited in scope, as it focuses on bodily privacy. It is rendered ineffective against non-sexual deepfakes, such as political misinformation or financial fraud, where

[2] Akshat Agarwal, "Director's Liability for AI Harms: A Fiduciary Perspective", *Tech Law Forum*, NALSAR (2025).
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[4] Information Technology Act, 2000, Section 66D (India).

the harm is reputational rather than physical.[5] Even in cases of "deepfake pornography" (NCII), if the base image used is a face (which is public) morphed onto a body that is not the victim's, the applicability of Section 66E is contested because the "private area" captured does not actually belong to the victim.

- **Sections 67 and 67A (Obscenity): These sections penalise** the transmission of obscene or sexually explicit material. While these have been the primary vehicles for prosecuting non-consensual deepfake pornography, they are dependent on community standards of "obscenity." They fail to cover "harmful but not obscene" content, such as a deepfake depicting a teetotaler politician drinking alcohol or using drugs, which are not illegal or obscene but are defamatory and damaging to specific reputations.[6]

1.2.2 The "Active Participant" Shift: Intermediary Liability and the IT Rules

A critical evolution in the Indian legal framework is the erosion of the "Safe Harbour" protection under Section 79 of the IT Act. Historically, intermediaries were immune from liability for third-party content if they acted as passive conduits. However, the rise of Generative AI has challenged this passivity.

Recent amendments to the **IT Rules, 2021 (specifically Rule 3(1)(b))** and subsequent advisories from the Ministry of Electronics and Information Technology (MeitY) have fundamentally altered this landscape. The rules now require intermediaries to "make reasonable efforts" to prevent users from hosting content that "impersonates another person" or is "patently false and untrue" (misinformation), including deepfakes.[7]

- **The Loss of Neutrality:** Legal scholars argue that GenAI platforms (like ChatGPT or Midjourney) cannot claim Section 79 protection because they are "active participants" in the content creation process. Unlike a social media host, a GenAI model *generates* content in response to prompts. Therefore, the safe harbour provision, designed for passive transmission, is arguably inapplicable to AI developers.[8]

[5] *Id.* at Section 66E.
[6] *Id.* at Section 67A.
[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, Rule 3(1)(b) (India).
[8] Rishabh Dara, "Intermediary Liability in India: Chilling Effects on Free Expression", *SSRN Electronic Journal* (2011).

- **Due Diligence Obligations:** The 2023 and 2024 advisories reinforce that failure to act on deepfakes within strict timelines (24 to 36 hours) results in the forfeiture of safe harbour immunity, exposing platforms to criminal liability under the Indian Penal Code (IPC).[9]

1.2.3 Judicial Evolution: From Static Images to AI Personas

Jurisprudence has evolved rapidly, shifting from protecting static images to protecting dynamic "personas" against AI emulation.

A. The Foundation: *Titan Industries v. Ramkumar Jewellers* (2012)

In *Titan Industries Ltd. v. M/S Ramkumar Jewellers*, the Delhi High Court laid down the seminal test for personality rights infringement. The case involved the unauthorised use of Amitabh Bachchan's image on hoardings. The court established three elements for liability:

1. **Validity**: The plaintiff owns an enforceable right in the identity.
2. **Identifiability**: The celebrity must be identifiable from the defendant's unauthorised use.
3. **Identity, not Confusion:** Crucially, the court held that no proof of falsity, confusion, or deception is required if the celebrity is identifiable.[10]

This "identifiability" test is critical for deepfakes. It suggests that even if a deepfake is labelled as "fake" (via a disclaimer), if the viewer *identifies* the subject as the celebrity, a violation of personality rights has occurred. This effectively counters the "parody defence" often used by deepfake creators, establishing a strict liability standard for commercial misuse of identity.

B. The Expansion: *Amitabh Bachchan v. Rajat Nagi* (2022)

As technology advanced, the courts recognised the need for broader protection. In *Amitabh Bachchan v. Rajat Nagi*, the Delhi High Court granted a "blanket John Doe order" (an *ad*

[9] Ministry of Electronics and Information Technology, "Advisory on Due Diligence by Intermediaries" (Dec. 2023)
[10] *Titan Industries Ltd. v. M/S Ramkumar Jewellers*, (2012) 50 PTC 486 (Del), at ¶ 12.

interim in rem injunction).[11]

- **Context**: Defendants were using Bachchan's voice and image for lottery scams and unauthorised merchandise.

- **Legal Innovation**: The court directed the Ministry of Electronics and Information Technology (MeitY) and Telecom Service Providers (TSPs) to block access to infringing content indiscriminately. This marked a shift from "notice-and-takedown" (reactive) to "blocking orders" (preventive), acknowledging that digital infringement spreads too fast for individual lawsuits.

- **Significance**: The court recognised that "personality attributes" (voice, mannerisms) are distinct intellectual property assets. This paved the way for the protection against AI voice cloning, even before deepfakes became a mainstream subject of litigation.[12]

C. The AI Turning Point: *Anil Kapoor v. Simply Life India* (2023)

The judgment in *Anil Kapoor v. Simply Life India & Ors.* is the most significant development in Indian personality rights law concerning AI.[13]

- **The Harm**: Defendants used AI to create "morphed" videos, GIFs, and "dark patterns" using Kapoor's likeness, and even claimed to use his voice for motivational speaking.

- **The Ruling**: Justice Prathiba M. Singh issued a comprehensive order protecting Kapoor's name, voice, image, and even his signature dialogue delivery ("Jhakkas") from "technological misuse".[14]

- **Key Doctrine - The Right to Livelihood**: The court explicitly linked personality rights to the "Right to Livelihood" under Article 21. It reasoned that a celebrity's persona is their primary source of income; therefore, AI-generated dilution

[11] *Amitabh Bachchan v. Rajat Nagi*, (2022) 6 HCC (Del) 641.
[12] Khushi Singh, "Position of Personality Rights in India: Amitabh Bachchan v. Rajat Nagi Case", *JusIP* (2024).
[13] *Anil Kapoor v. Simply Life India & Ors.*, CS(COMM) 652/2023 (Del HC, Sept. 20, 2023).
[14] Pallavi Tiwari, "Anil Kapoor v. Simply Life India & Ors.: Perspective of Indian Judiciary", *Vishwakarma University Law Journal*, Vol. IV (2024).

of that persona is a threat to their economic survival.[15]

- **AI Specifics**: The order specifically restrained the use of "Artificial Intelligence," "deepfakes," and "morphing" technologies to create derivative works. It acknowledged that AI tools enable a form of infringement qualitatively distinct from simple copyright theft: **identity theft** at scale.

Critique: While the *Anil Kapoor* judgment is progressive, it relies heavily on interim injunctions. There is currently no statutory definition of "personality rights" in India. Critics argue that these "ex parte" injunctions may overprotect fame at the cost of free speech (e.g., banning satire or memes).[16] Furthermore, these protections are broadly accessible only to celebrities with the resources to litigate, leaving ordinary citizens vulnerable to deepfake abuse without a straightforward "personality right" remedy.[17]

1.3 IPR-Specific Challenges: Copyright, Training Data, and Trademark Dilution

The intersection of AI and Intellectual Property Rights (IPR) gives rise to two distinct conflicts: the "input" side (the use of data to train AI) and the "output" side (the deepfake itself infringing on rights).

1.3.1 Copyright Infringement in AI Training Data

Deepfake models require vast datasets of images and audio to "learn" a person's likeness. The legal status of scraping this data is the subject of the landmark suit *ANI v. OpenAI*.[18]

- **The ANI v. OpenAI Case**: Asian News International (ANI) sued OpenAI, alleging that ChatGPT was trained on its copyrighted news articles and videos without a license. ANI argued that this constitutes "reproduction" under Section 14 of the Copyright Act. This case is India's first significant test of copyright law regarding GenAI training practices.[19]

[15] *Id.* at 3.
[16] "Personality Rights: The Law Must Not Overprotect Fame", *Supreme Court Observer* (2024).
[17] "The Mirage of Fame: Deepfakes, AI and Evolving Jurisprudence", *IIPRD Blog* (2024).
[18] *Asian News International (ANI) v. OpenAI Inc.*, CS(COMM) 2024 (Del HC).
[19] Dyuti Pandya, "The Global South AI Copyrights Test Case: India", *CEPA* (Mar. 7, 2025).

- **The "Storage Paradox"**: A key legal question is whether the *temporary* storage of data in a neural network's weights constitutes "storage" under copyright law. Some scholars argue that once the AI "learns" the pattern, the original data is discarded and the model retains only abstract numerical representations (weights).[20] However, if the AI can reproduce the data *verbatim* (or generate a perfect likeness of an ANI anchor), it suggests the original expression is effectively stored and reproduced, violating the exclusive rights of the copyright owner.

- **Fair Dealing Defence**: Unlike the US concept of "Fair Use," India's "Fair Dealing" under Section 52 is exhaustive and specific. It allows exceptions for "research," "criticism," and "review," but does not explicitly exempt "machine learning" or "text and data mining" (TDM) for commercial purposes.[21] This suggests that, under a strict doctrinal reading, training commercial AI models on copyrighted celebrity images without a license constitutes infringement. The absence of a specific TDM exception, unlike in the EU or Singapore, leaves Indian AI developers in a precarious legal position and victims of data scraping with a strong theoretical claim.

1.3.2 Trademark Dilution and False Endorsement

Deepfakes often function as "False Endorsements," leading consumers to believe a celebrity supports a product.

- **Passing Off vs. Deepfakes**: The tort of passing off protects goodwill. In *Titan Industries*, the court held that an unauthorised endorsement misleads the public. However, deepfakes complicate the "misrepresentation" element. If a deepfake is perfect, the consumer is *genuinely* deceived. If the deepfake is poor or labelled "parody," the consumer is arguably not deceived. Yet, the harm persists.

- **The "Dilution" Theory**: The *Anil Kapoor* judgment recognised "dilution by tarnishment". Even if no one believes Anil Kapoor actually endorsed a pornographic video (due to context), the mere association tarnishes his brand. This moves Indian law

[20] "ANI v. OpenAI: The Storage Paradox is More Than Just Transient", *SpicyIP* (May 2025).
[21] "AI Training or Copyright Infringement: Drawing Parallels Between US and Indian Perspective", *Legal Era* (2025).

closer to the U.S. concept of trademark dilution, protecting the mark's (persona) dignity rather than merely consumer confusion.[22]

- **Generic Deepfakes**: A major inadequacy is the lack of protection for non-celebrities. Trademark law requires "goodwill" or "commercial reputation." An ordinary woman whose face is deepfaked into a pornographic video cannot sue for "passing off" as she has no commercial "brand" to dilute. This leaves a significant gap in which IPR fails to protect the dignity of private citizens, necessitating a privacy-based approach.

1.4 Privacy and Consent Issues: The DPDP Act, 2023

The **Digital Personal Data Protection (DPDP) Act, 2023**, introduces a new statutory regime that could, in theory, regulate deepfakes, provided that synthetic data is recognised as "personal data."

1.4.1 Deepfakes as "Inaccurate Personal Data"

- **Definition**: Section 2(t) defines "personal data" as any data about an identifiable individual. A deepfake uses biometric features (face, voice), which are inherently personal[23].

- **Accuracy Obligation**: Section 8(3) mandates Data Fiduciaries (platforms) to ensure the "completeness, accuracy, and consistency" of personal data. A deepfake, by definition, is a *fabrication*. Therefore, a platform hosting a deepfake of a user is processing "inaccurate personal data." This gives the victim the **Right to Correction and Erasure** (Section 12), allowing them to demand the removal of the false representation.[24]

- **Consent and Purpose Limitation**: The Act requires consent for processing. A user may consent to uploading their photo to Instagram, but they do not consent to that photo being scraped for use in training a deepfake model. This "purpose limitation"

[22] Joshua Beser, "False Endorsement or First Amendment", 41 *San Diego L. Rev.* 1787 (2004).
[23] Digital Personal Data Protection Act, 2023, Section 2(t) (India).
[24] *Id.* at Section 12.

violation is a strong legal hook for challenging AI scrapers.[25]

1.4.2 The "Publicly Available" Loophole

A critical weakness in the DPDP Act is the potential exemption for data "made publicly available by the Data Principal" (Section 3(c)).

- **The Problem**: If a person posts their own photo on a public Twitter profile, does the DPDP Act cease to apply? If so, deepfake creators could argue that scraping public profiles is lawful.

- **Legal Counter-Argument**: Even if the data is public, the *processing* (creating a deepfake) creates *new* data (the synthetic video) that is false. The exemption for public availability should not extend to the creation of *false* derivatives that harm the individual's reputation. The *Anil Kapoor* judgment supports this, ruling that "public availability" does not imply a license to exploit.[26]

1.4.3 Biometric Data and "Sensitive" Processing

While the DPDP Act removes the distinction between "sensitive" and "ordinary" personal data (unlike the GDPR), the government has the power to notify "Significant Data Fiduciaries" (SDFs). Platforms that host AI content may be classified as SDFs, subjecting them to higher compliance standards, including Data Protection Impact Assessments (DPIAs).[27] However, without specific rules on AI, the Act remains a "paper tiger" regarding deepfake regulation.

1.5 Enforcement Barriers: The Jurisdictional Quagmire

Even with robust substantive laws, enforcement against deepfakes is hampered by procedural hurdles, primarily attributable to the internet's borderless nature.

1.5.1 Intermediary Liability and the "Safe Harbour" Erosion

Section 79 of the IT Act provides a "safe harbour" to intermediaries (ISPs and social media

[25] "Deepfakes, Privacy and Data Protection in India", *Lex Scripta Magazine* (Jan. 2026).
[26] *Anil Kapoor v. Simply Life India & Ors.*, CS(COMM) 652/2023.
[27] Digital Personal Data Protection Act, 2023, Section 10 (India).

platforms) if they act as passive conduits.

- **The "Active Participant" Shift**: Generative AI platforms (like Midjourney or ChatGPT) are not "passive conduits." They *create* content in response to user prompts. Legal scholars and recent advisory opinions suggest that GenAI platforms are not entitled to Section 79 protection because they are "active participants" in the content creation process.[28]

- **Rule 3(1)(b) Amendments**: The IT Rules, 2021 (amended in 2023) mandate intermediaries to "make reasonable efforts" to prevent users from uploading deepfakes (impersonation).[29] Failure to do so risks loss of safe harbour.

- **Enforcement Reality**: While the law is clear, the sheer volume of content makes preemptive filtering technologically difficult without high false positives. Furthermore, platforms often delay takedowns, citing "jurisdictional" issues when a request originates from Indian authorities but the server is in the US.

1.5.2 Cross-Border Jurisdiction and MLAT Failures

Deepfake crimes are often transnational: the victim is in India, the perpetrator in Eastern Europe, and the server in the US.[30]

- **Mutual Legal Assistance Treaties (MLATs)**: Obtaining evidence (IP logs) from foreign jurisdictions relies on MLATs. The average time for an MLAT response in India is **3 years and 4 months**.[31] In deepfake cases, where viral spread happens in minutes, this delay renders the mechanism useless.

- **Data Localisation: The lack of mandatory data localisation** for non-payment data means Indian law enforcement has no direct access to server logs, forcing them to rely on voluntary cooperation from Big Tech, which is inconsistent.

1.5.3 The "Digital India Act" and Future Regulation

The proposed **Digital India Act (DIA)** aims to address these gaps by defining "high-risk AI"

[28] "India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship", *Tech Policy Press* (2025).
[29] Ministry of Electronics and Information Technology, "Press Note: Deepfake Regulation", *PIB* (Dec. 2025).
[30] Cross-Border Cybercrimes: Challenges in Jurisdiction and Enforcement", *Vox Legis* (2025).
[31] "Building Law Enforcement Capacity to Tackle Cyber Threats", *ORF* (2025).

and potentially mandating "algorithmic accountability".[32]

- **Definition of Harm**: The DIA draft considers defining "harm" to include "misinformation" and "impersonation," which would directly target deepfakes.

- **Algorithmic Accountability**: The act may require platforms to disclose their algorithms and ensure they are not biased or prone to generating harmful content.[33]

1.6 Novel Framework: "Deepfake Torts" and Corporate Vicarious Liability

Given the inadequacies of the "notice-and-takedown" model and the "whack-a-mole" nature of suing anonymous users, this report proposes a novel legal framework: **Deepfake Torts under Company Law**. This approach shifts liability from the *AI user to the corporate creator of the AI, invoking* principles of hazardous liability.

1.6.1 The Theory of "Deepfake Torts"

We propose recognising a new category of torts specifically for harms caused by AI systems that lack adequate safety guardrails. This is grounded in the "Duty of Care" principle.

- **Foreseeability**: It is foreseeable that a high-fidelity voice cloning tool will be used for fraud.

- **Proximity**: The AI developer is the only entity capable of embedding safeguards (e.g., watermarks, C2PA provenance).

- **Liability**: If an AI developer releases a tool without these safeguards, they should be liable for the resultant harms, distinct from the user's criminal liability.[34]

1.6.2 Vicarious Liability of AI Firms

Under standard corporate law, a company is vicariously liable for the acts of its agents.

- **AI as "Agent"**: Scholars argue that autonomous AI agents function analogously to employees. If an AI "hallucinates" a defamatory statement (as in *ANI v.*

[32] "Digital India Act: Draft Framework for AI Regulation", MeitY
[33] "India's Advance on AI Regulation", Carnegie Endowment (Nov. 2024).
[34] Companies Act, 2013, Section 166 (India).

OpenAI) or generates a deepfake that bypasses safety filters, the corporation should be liable for "defective supervision" of its digital agent.

- **Director's Liability (Section 166, Companies Act 2013)**: Directors have a fiduciary "duty to exercise reasonable care, skill, and diligence." In the age of AI, this must include **Algorithmic Risk Assessment**.[35] We argue that failing to implement "Safety by Design" (e.g., preventing the generation of NCII) constitutes a breach of fiduciary duty, exposing directors to class action lawsuits by victims of deepfakes generated by their tools.

1.6.3 Applying *M.C. Mehta* (Absolute Liability) to AI

The most radical but necessary legal innovation is applying the **Absolute Liability** principle from *M.C. Mehta v. Union of India* (the Oleum Gas Leak case) to Generative AI.[36]

- **The Principle**: An enterprise engaged in a "hazardous or inherently dangerous" activity is absolutely liable to compensate for any harm caused, regardless of negligence.[37]

- **Application**: Generative AI, capable of destroying reputations and destabilising democracies (elections), meets the threshold of "inherently dangerous." Therefore, AI labs should be held strictly liable for harms caused by their models, thereby incentivising them to "internalise the externalities" of their technology. This moves beyond "Strict Liability" (which permits exceptions) to a regime in which the mere occurrence of harm triggers corporate liability.

1.6.4 Remedy: Algorithmic Disgorgement

When liability is established, monetary damages are often insufficient to restore dignity. We propose the remedy of **Algorithmic Disgorgement** (or Model Deletion).

- **Concept**: If an AI model is found to be trained on infringing data (e.g., unauthorised celebrity images) or is deemed "hazardous," the court should order the

[35] *M.C. Mehta v. Union of India*, AIR 1987 SC 1086.
[36] "Strict Liability and Absolute Liability in Indian Perspective", *International Journal of Law Management & Humanities* (2024).
[37] Tiffany C. Li, "Algorithmic Destruction", 75 *SMU L. Rev.* 479 (2022).

deletion of the model itself, not just the data.

- **Legal Basis**: This remedy has been used by the US FTC (e.g., Everalbum case) and aligns with the Indian concept of "destruction of infringing goods" under IPR laws. It ensures that the "fruit of the poisonous tree" (the trained neural network) is removed from commerce.[38]

Conclusion

The legal challenges in protecting personality rights from deepfakes are systemic, stemming from a disconnect between 20th-century statutes and 21st-century technology. While judicial activism in cases like *Anil Kapoor* has provided temporary relief, a structural overhaul is required. This involves:

1. **Statutory Recognition**: Amending the Copyright Act to define "digital persona" rights explicitly.

2. **Strict Liability**: Enacting "Deepfake Tort" provisions that hold AI platforms accountable as manufacturers of hazardous products, not just passive intermediaries.

3. **Algorithmic Accountability**: Mandating "disgorgement" of models trained on stolen identity data.

Only by treating deepfakes not as "content" but as "hazardous products" can the Indian legal system hope to protect the integrity of human personality in the digital age.

[38] "In the Sidelines of the AI Conversation: Model Disgorgement and Algorithm Deletion", *Asia IP* (2025).

BIBLIOGRAPHY

Statutes, Bills, and Regulations

- Companies Act, 2013 (Specifically Section 166).
- Constitution of India (Specifically Article 21).
- Copyright Act (Specifically Sections 14 and 52).
- Digital India Act (DIA) (Proposed).
- Digital Personal Data Protection (DPDP) Act, 2023 (Specifically Sections 2(t), 3(c), 8(3), and 12).
- Indian Penal Code (IPC).
- Information Technology Act, 2000 (Specifically Sections 66D, 66E, 67, 67A, and 79).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Specifically Rule 3(1)(b)).

Table of Cases (Indian)

- *Amitabh Bachchan v. Rajat Nagi* (2022).
- *ANI v. OpenAI*.
- *Anil Kapoor v. Simply Life India & Ors*. (2023).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*.
- *M.C. Mehta v. Union of India*.
- *Titan Industries Ltd. v. M/S Ramkumar Jewellers* (2012).

Table of Cases (International / Foreign Agency)

Everalbum case (US Federal Trade Commission)