Page 2473 - 2489 **DOI:** *https://doi.org/10.63108/IJLMH.12728*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

AI-Generated Deepfakes in India: Consent, Privacy, and the Limits of Existing Cyber Regulation

ISHAAN BHARDWAJ[*] AND DR. ANUSHREE MUKTE[**]

ABSTRACT

Artificial intelligence is no longer a one-way instrument embedded within digital systems. It now shapes how people relate to one another, and its absorption into data governance marks a shift from artificial intelligence as a component of digital infrastructure to artificial intelligence as a means of governing that infrastructure, and with it a part of ordinary human experience. The shift is troubling chiefly because it has made hyper-realistic synthetic images, audio and video cheap to produce, and such material displaces a person's face, voice and likeness. Deepfakes are images, videos and voice recordings of people, living and deceased, whose faces and voices have been altered without their agreement. This paper takes a doctrinal approach and argues that the Indian framework governing synthetic media suffers from legal lag. It assesses the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023, and finds that neither parent statute defines synthetic media, that the labelling and provenance duties introduced in February 2026 sit in subordinate legislation rather than in the statute book, that the identity offences on which prosecutors must rely were drafted for the misuse of existing credentials and not for the fabrication of a likeness, and that the substantive obligations of the data protection statute are not yet in force. It considers India's decision not to accede to the Budapest Convention on Cybercrime and the consequences for cross-border evidence collection, and it compares the regulatory regimes of the European Union, the United States, the United Kingdom and China. The paper calls for targeted legislative measures on the model of those jurisdictions: a statutory definition of synthetic media, mandatory labelling, and a fast track for statutory takedown. Three changes are treated as crucial: takedown timeframes with a statutory footing, a victim-centred reporting framework, and sustained public education. The position is stated as at August 2026.

Keywords: *Deepfakes, Artificial Intelligence, Digital Consent, Synthetic Media, Personality Rights, Information Technology Act 2000, Digital Personal Data Protection Act 2023, Budapest Convention, Cyber Regulation, Privacy*

[*] Author is a Second Year BA LLB Student at Symbiosis Law School, Nagpur, Maharashtra, India.
[**] Author is an Assistant Professor at Symbiosis Law School, Nagpur, Maharashtra, India.

 [ISSN 2581-5369]

I. INTRODUCTION

Until the digital revolution, societies operated largely on real-world records, on dealings conducted in person, and on traditional methods of storing and organising information. Research, data management and communication were slow, and were bounded by human capacity. Digital technologies transformed those processes by making information readily available and interconnected. Artificial intelligence is the next advance on that platform. Where the digital era was concerned chiefly with storing and sharing information, artificial intelligence supplies systems that analyse data, identify patterns and act with little human intervention. It may therefore be understood as the next generation of the digital age, one in which technology ceases to be a passive bystander to human life and becomes a constituent part of it.

As a field of computer science, artificial intelligence has been developing since the 1950s. Its foundational statement is generally traced to Alan Turing, the British mathematician and cryptanalyst, who proposed what he called the imitation game, now commonly known as the Turing test, as a way of assessing whether a machine could exhibit behaviour indistinguishable from that of a human.[1] The Dartmouth Summer Research Project on Artificial Intelligence, proposed in 1955 by John McCarthy, Marvin Minsky, Nathaniel Rochester and Claude Shannon and held the following summer, gave the field both its name and its independent identity.[2] In its earliest stage the discipline relied on fixed rules and predetermined objectives written by developers. The later development of machine learning marked a departure, machine learning being a form of artificial intelligence in which computers use large volumes of data to learn how to perform a task rather than being programmed to perform it.[3]

Performance therefore improves with exposure to more data. Artificial intelligence, broadly understood, is the simulation of human intelligence by machines capable of learning, reasoning and self-correction. Among the applications of that capability, the generation of deepfakes has proved the most contested. Deepfakes are images, audio and video produced by training models on large volumes of material, and the better examples reproduce expression and small involuntary movement closely enough that an exchanged face, an altered expression or a cloned voice reads as genuine.

---

[1] A.M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950), https://doi.org/10.1093/mind/LIX.236.433.

[2] John McCarthy, Marvin L. Minsky, Nathaniel Rochester & Claude E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*, 27 AI MAGAZINE 12 (2006).

[3] *Machine Learning*, OXFORD ADVANCED LEARNER'S DICTIONARY, https://www.oxfordlearnersdictionaries.com/definition/english/machine-learning (last visited Aug. 19, 2026).

 [ISSN 2581-5369]

This paper addresses three questions. First, what gaps does the Digital Personal Data Protection Act 2023 leave in relation to AI-generated deepfakes? Second, what consequences follow, for the investigation and prosecution of deepfake offences, from India's decision not to accede to the Budapest Convention on Cybercrime? Third, what lessons can be drawn from comparative practice, and what legislative and institutional reforms would equip India to act on them?

The method is doctrinal. The paper examines the relevant provisions of the Information Technology Act 2000[4] and the Digital Personal Data Protection Act 2023,[5] the subordinate legislation made under the former, and the recent Indian decisions on AI-generated content and personality rights. It sets these against the regulatory regimes of the European Union, the United States, the United Kingdom and China, and it draws on credible news reportage to show how synthetic media operates in practice. The enquiry is confined to legal and regulatory questions, and offers no technical assessment of detection tools. Its focus is the effect of AI-generated deepfakes on consent, privacy and digital security in India. This is a fast-moving field, and the position is stated as at August 2026.

II. ARTIFICIAL INTELLIGENCE, DIGITAL DATA, AND DEEPFAKES

Artificial intelligence has changed how data is created, stored and protected. Systems now generate text, images, video and software, and raise measured productivity across sectors. Survey evidence collected by researchers at the Federal Reserve Board indicates that between twenty and forty per cent of workers report using artificial intelligence at work, with markedly higher rates in technical occupations such as computer programming.[6]

The gains are not confined to content generation. Organisations use these systems for indexing, sorting and retrieval across large repositories, and their predictive capacity supports better storage allocation and automation. In cybersecurity the same techniques detect anomalies, identify threats and respond to them in real time, protect critical information, alert response teams and assist in the recovery of lost data. Efficiency, reduced operating cost, greater accuracy and scalability together explain the speed of adoption, and they have made artificial intelligence a working part of data governance and of digital transformation generally.

Reliance of that order carries risk. Public data is by definition accessible, but private data requires protection if an individual is to retain control over information about himself or herself. When these systems reach private data, the resulting processing is non-consensual and the harm

[4] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000) (India).
[5] The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023) (India).
[6] Leland D. Crane, Michael Green & Paul E. Soto, *Measuring AI Uptake in the Workplace*, FEDS NOTES (Feb. 5, 2025), https://doi.org/10.17016/2380-7172.3724.

 [ISSN 2581-5369]

falls directly on privacy. The same tools have lowered the cost of misuse, opening new avenues by which bad actors extend the reach and the impact of their conduct. It is this risk that calls for specific statutory regulation.

Deepfakes are hyper-realistic synthetic media, AI-generated depictions of faces, voices and bodies that appear to belong to real people.[7] Their social effects are broad, extending to electoral manipulation, financial fraud and questions of platform accountability, and they have provoked a continuing legal debate about the protection of privacy and dignity. The question is whether the existing Indian framework, principally the Information Technology Act 2000[8] and the more recent Digital Personal Data Protection Act 2023,[9] is adequate in scope to the harm now being documented.

A. Documented harms and the judicial response

The pattern is visible in a series of reported incidents. In November 2023 a video circulated widely online in which, according to contemporaneous reporting, the face of the actor Rashmika Mandanna had been superimposed on footage originally posted by another woman. The Delhi Police are reported to have registered a first information report on 10 November 2023 under sections 465 and 469 of the Indian Penal Code and sections 66C and 66E of the Information Technology Act, and an arrest was reported in January 2024.[10,11]

A case reported in May 2026 shows the same conduct outside the entertainment industry. Press reports state that a man was arrested by the cyber crime branch at Ahmedabad after allegedly opening about ten fraudulent social media accounts in the name of a woman whose approach he had made online and who had declined it, and uploading more than a hundred AI-generated nude images of her and of her mother, the material having been produced with freely available tools that purport to remove clothing from photographs. The offences invoked are reported to be sections 78(2) and 356(2) of the Bharatiya Nyaya Sanhita and sections 66C and 67 of the

[7] Zeeshan Shaikh, Eashaan Ambasana, Moiz Morbiwala & Vidya Sagvekar, *Exploring Legal and Technical Challenges of Deepfake in India*, 13 INT'L J. FOR RSCH. IN APPLIED SCI. & ENG'G TECH. 124 (2025), https://doi.org/10.22214/ijraset.2025.68385.

[8] The Information Technology Act, *supra* note 4.

[9] The Digital Personal Data Protection Act, *supra* note 5.

[10] *Rashmika Mandanna Calls for Action Against 'Scary' Deepfake Video*, BBC NEWS (Nov. 7, 2023), https://www.bbc.com/news/world-asia-india-67305557.

[11] *Andhra Man Held for Creating Rashmika Mandanna Deepfake Video, Wanted to Increase Followers*, NEWSMETER (Jan. 20, 2024), https://newsmeter.in/top-stories/creator-of-deepfake-video-of-actor-rashmika-mandanna-arrested-says-delhi-police-723573.

 [ISSN 2581-5369]

Information Technology Act.[12] The victims in such cases are private individuals, and the reporting does not identify them.

The reach of the harm is not confined to entertainers. In *Dr Devi Prasad Shetty v. Medicine Me*, the Delhi High Court granted ex parte ad interim relief to a cardiac surgeon and to the hospital group he founded, restraining the misuse of his name, likeness, image, photographs and videos, including through the use of any existing or future technology such as artificial intelligence and deepfake technology, and directing the platform intermediaries before it to disable access to the listed uniform resource locators.[13] The order is interim and its reasoning largely records the plaintiffs' submissions, but the relief granted shows that a medical practitioner in ordinary professional life may need the same protection as a film actor.

The doctrinal response of the Indian courts has developed cumulatively rather than through any single legislative intervention. Its constitutional foundation was laid in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which a nine-judge Bench of the Supreme Court held privacy to be a fundamental right intrinsic to Article 21.[14,15] That holding is the bedrock on which the later personality rights jurisprudence has been built.

Against that background, the singer Arijit Singh complained that his voice had been synthesised and made commercially available without his consent, and in July 2024 the Bombay High Court granted an ad interim injunction restraining the use of his name, voice, vocal style and technique, manner of singing, photograph, likeness, signature and persona. The order extends in terms to the use of those attributes through artificial intelligence voice models, voice conversion tools, synthesised voices and digital avatars, and across physical, digital and metaverse media.[16]

That order was preceded by the Delhi High Court's order in *Anil Kapoor v. Simply Life India*, made in a commercial suit on 20 September 2023, which was among the first Indian orders to name artificial intelligence, machine learning, deepfakes and face morphing expressly as the technological means by which personality rights were being infringed.[17] The same court

[12] *Delhi Man Made 100 AI Nude Photos, Videos of Influencer After Rejection, Arrested*, INDIA TODAY (May 28, 2026), https://www.indiatoday.in/india/story/ai-generated-nude-photos-delhi-man-held-ahmedabad-influencer-mother-2918567-2026-05-28.
[13] *Dr Devi Prasad Shetty v. Medicine Me*, 2024 SCC OnLine Del 8565, CS(COMM) 1053/2024 (Del. H.C. Nov. 28, 2024) (India).
[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[15] INDIA CONST. art. 21.
[16] *Arijit Singh v. Codible Ventures LLP*, 2024 SCC OnLine Bom 2445, Com. IPR Suit (L) No. 23443 of 2024 (Bom. H.C. July 26, 2024) (India).
[17] *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914, CS(COMM) 652/2023 (Del. H.C. Sept. 20, 2023) (India).

 [ISSN 2581-5369]

extended the protection in *Jaikishan Kakubhai Saraf v. The Peppy Store*, where an unlicensed artificial intelligence chatbot deploying the actor's persona was among the uses restrained. That order also marks the limit of the doctrine, because the court declined to restrain a satirical video, treating meme and parody content as protected expression notwithstanding the commercial benefit it generated.[18]

An earlier order in the same line, *Amitabh Bachchan v. Rajat Nagi*, restrained the unauthorised commercial use of the actor's name, likeness, photograph and voice in connection with fraudulent lottery schemes conducted in his name.[19] It is an important step in the development of the doctrine, although it says nothing about synthetic media, and it should not be read as a deepfake authority.

These orders are doctrinally notable because the courts have treated publicity and personality rights as enforceable common law rights against impersonation by artificially generated imagery, and have begun in that way to fill a gap the legislature has not closed. Taken with the reported incidents, they show both the scale of the harm that deepfake technology facilitates and its uneven distribution across women, professionals and private citizens.

B. Political manipulation and the erosion of the evidentiary record

Synthetic media has also entered electoral politics. Al Jazeera reported that on 23 January 2024 an AI-generated likeness of the late M. Karunanidhi, formerly Chief Minister of Tamil Nadu, who died in 2018, appeared on a projected screen before a live audience and delivered an address of some eight minutes praising the present leadership of his party, and that this was the third such reanimation in six months.[20] The material was produced openly and was not presented as a forgery, but it illustrates how readily the technology can be turned to campaigning.

In the United States, automated calls using a synthesised imitation of the voice of President Joseph Biden reached New Hampshire voters shortly before the state primary in January 2024, urging them not to vote.[21] The regulatory and the criminal responses then diverged instructively. The Federal Communications Commission finalised a forfeiture of six million

[18] *Jaikishan Kakubhai Saraf v. The Peppy Store*, 2024 SCC OnLine Del 3664, CS(COMM) 389/2024 (Del. H.C. May 15, 2024) (India).
[19] *Amitabh Bachchan v. Rajat Nagi*, 2022 SCC OnLine Del 4110, CS(COMM) 819/2022 (Del. H.C. Nov. 25, 2022) (India).
[20] Nilesh Christopher, *How AI Is Resurrecting Dead Indian Politicians as Election Looms*, AL JAZEERA (Feb. 12, 2024), https://www.aljazeera.com/economy/2024/2/12/how-ai-is-used-to-resurrect-dead-indian-politicians-as-elections-loom.
[21] Max Matza, *Fake Biden Robocall Tells Voters to Skip New Hampshire Primary Election*, BBC NEWS (Jan. 22, 2024), https://www.bbc.com/news/world-us-canada-68064247.

 [ISSN 2581-5369]

dollars in September 2024 against the political consultant who had commissioned the calls,[22] while a New Hampshire jury acquitted him of all criminal charges in June 2025, the defence contending that the voter suppression statute did not apply to a primary and that no candidate had been impersonated because none was named.[23] Both episodes share a vulnerability. Whatever the regulatory context, synthetic media can taint an electoral process well before any liability attaches to its maker.

Journalism and media organisations face a related pressure. Verification consumes an increasing share of editorial resources, and the resulting delay is itself a cost. Deepfakes have also produced what has been described as the liar's dividend, a condition in which audiences grow less willing to believe what they see, and in which that scepticism allows a wrongdoer to dismiss genuine evidence as a fabrication.[24]

III. THE INDIAN LEGAL FRAMEWORK AND ITS REGULATORY GAPS

Having considered the technology and its social consequences, it is necessary to ask whether Indian law has kept pace with it. Social change of this order ordinarily calls for legislative response. Two statutes carry the burden: the Information Technology Act 2000, which governs computer systems, data and electronic privacy, and the Digital Personal Data Protection Act 2023. Neither contains a definition of a deepfake, a synthetic image or an AI-generated work. In the absence of any statutory definition the judiciary has had to resolve disputes over the technology through traditional doctrinal routes, and a framework built for harms that were understood when the statutes were drafted is structurally ill-suited to harms that emerged afterwards. The regulatory shortcomings that follow from this are set out below.

A. Identity offences under the Information Technology Act

The Information Technology Act 2000 contains several provisions of potential relevance to deepfake harms. Section 66C penalises the fraudulent or dishonest use of the electronic signature, password or any other unique identification feature of another person, and is punishable with imprisonment for a term which may extend to three years together with a fine which may extend to one lakh rupees.[25] The provision is built around the misappropriation of credentials that already exist. It does not contemplate the creation of synthetic content that

[22] *Consultant Fined $6 Million for Using AI to Fake Biden's Voice in Robocalls*, REUTERS (Sept. 26, 2024), https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/.
[23] Holly Ramer, *New Hampshire Jury Acquits Consultant Behind AI Robocalls Mimicking Biden on All Charges*, ASSOCIATED PRESS (June 13, 2025), https://apnews.com/article/ai-robocalls-new-hampshire-biden-kramer-e87ef8848a2a6515202535a6e800da07.
[24] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019).
[25] The Information Technology Act, No. 21 of 2000, s. 66C, INDIA CODE (2000) (India).

 [ISSN 2581-5369]

fabricates a likeness without relying on any credential at all. Section 66D penalises cheating by personation by means of a computer resource, and carries the same maximum sentence and fine.[26] It is the closer fit of the two, because a convincing deepfake is a personation, but it requires cheating, so it reaches the fraudster and not the person who circulates a fabricated intimate image for its own sake.

Section 66E penalises the intentional or knowing capture, publication or transmission of the image of a private area of a person without that person's consent, in circumstances violating that person's privacy, and is punishable with imprisonment which may extend to three years or with a fine not exceeding two lakh rupees, or with both.[27] The section turns on the capture of an image of a real body, and none of its explanations addresses a synthetic depiction, an omission that risks leaving non-consensual deepfake pornography outside the provision altogether. Sections 67 and 67A, which penalise the publication and transmission of obscene material and of material containing a sexually explicit act in electronic form, are drafted without reference to the origin of the material and can therefore be applied to synthetic content, but they protect public decency rather than the individual whose likeness has been taken.[28] Section 66F addresses cyber terrorism and the conduct constituting it, and makes no reference to the creation of deepfakes intended to influence electoral outcomes through politically motivated disinformation.[29]

Section 79 confers the safe harbour on which the whole intermediary regime rests, exempting an intermediary from liability for third party information where it performs a mere conduit function or does not initiate the transmission, select the receiver or select or modify the information, and where it observes due diligence and the guidelines made by the Central Government.[30] The exemption falls away under section 79(3)(b) where the intermediary, on receiving actual knowledge, fails to remove the material expeditiously. In *Shreya Singhal v. Union of India* the Supreme Court read that clause down so that actual knowledge means a court order or a notification by the appropriate Government, and confined it to the grounds in Article 19(2).[31] The consequence for a deepfake victim is that a platform is under no general obligation to act on a private complaint alone unless the subordinate legislation says otherwise.

[26] *Id.* s. 66D.
[27] *Id.* s. 66E. The Explanation defines a private area as the naked or undergarment clad genitals, pubic area, buttocks or female breast.
[28] *Id.* ss. 67, 67A.
[29] *Id.* s. 66F.
[30] *Id.* s. 79.
[31] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, para. 119 (India).

 [ISSN 2581-5369]

The general criminal law is in the same position. The Bharatiya Nyaya Sanhita 2023 contains no deepfake-specific offence. A prosecutor must fall back on cheating by personation under section 319, forgery of a false electronic record under section 336, defamation under section 356, the provision on insulting the modesty of a woman and intruding upon her privacy under section 79, and the obscenity provisions in sections 294 and 295, which now expressly extend to the display of content in electronic form.[32] Each of these can be made to reach some part of the conduct, and none of them was drafted with a fabricated likeness in mind.

B. Subordinate legislation and the turn to labelling

The regulatory movement in India has occurred not in the statutes but beneath them. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 impose due diligence duties on intermediaries, including a duty under rule 3(2)(b) to remove, on complaint, material that exposes a person's private area, shows that person in full or partial nudity or in a sexual act, or is in the nature of impersonation in electronic form including artificially morphed images.[33] From November 2023 the Ministry of Electronics and Information Technology issued a series of advisories on deepfakes and on artificially generated content, of which the advisory of 15 March 2024 is the operative one, requiring the labelling of fallible output and the embedding of permanent unique metadata or identifiers in the output of deepfake-capable tools.[34] Advisories, however, are not law, and they had no independent sanction beyond the loss of safe harbour.

That changed on 20 February 2026, when the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 came into force.[35] Rule 2(1)(wa) now defines synthetically generated information as audio, visual or audio-visual information artificially or algorithmically created, generated, modified or altered using a computer resource in a manner that makes it appear real, authentic or true and that depicts a person or an event so as to be, or to be likely to be perceived as, indistinguishable from a natural person or a real-world event, subject to provisos excluding good faith editing, routine document preparation and

[32] The Bharatiya Nyaya Sanhita, No. 45 of 2023, ss. 79, 294, 295, 319, 336, 356, INDIA CODE (2023) (India).
[33] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(i), G.S.R. 139(E) (Feb. 25, 2021) (India), as amended by G.S.R. 794(E) (Oct. 28, 2022), G.S.R. 275(E) (Apr. 6, 2023) and G.S.R. 775(E) (Oct. 22, 2025).
[34] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Advisory No. 2(4)/2023-CyberLaws-3 (Mar. 15, 2024) (India), superseding the advisory of the same number dated Mar. 1, 2024; MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Advisory No. 2(4)/2023-CyberLaws-2 (Dec. 26, 2023) (India). The earlier advisory of Nov. 7, 2023 on deepfakes was announced by PRESS INFORMATION BUREAU Release No. 1975445 (Nov. 7, 2023) (India).
[35] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India, pt. II sec. 3(i), G.S.R. 120(E) (Feb. 10, 2026) (India) (in force Feb. 20, 2026), rr. 2(1)(wa), 3(3), 4(1A).

 [ISSN 2581-5369]

accessibility uses. Rule 3(3) requires intermediaries to deploy technical measures against unlawful synthetic content, to label such content prominently and to embed permanent metadata or provenance information including a unique identifier so far as is technically feasible, and forbids the removal or suppression of that label. Rule 4(1A) requires a significant social media intermediary to obtain a user declaration as to whether uploaded content is synthetically generated and to deploy technical measures to verify it. The takedown clocks were shortened at the same time: removal on actual knowledge under rule 3(1)(d) moved from thirty six hours to three, and removal of non-consensual intimate or impersonated imagery under rule 3(2)(b) moved from twenty four hours to two.[36]

India therefore now has AI-specific regulation, and the argument that no Indian instrument addresses synthetic media can no longer be made. What can be said, and what matters more, is that the definition and the duties live in delegated legislation made under section 87 of a statute that has itself not been amended. They can be altered by notification, they carry no criminal sanction of their own, and they bind intermediaries rather than the makers of the content. Nothing in them creates a cause of action for the person whose likeness has been taken.

The Digital Personal Data Protection Act 2023 does not fill that space either, and its position is often overstated. The Act contains no provision on synthetic media, deepfakes or AI-generated content. It does not apply at all to personal data that the data principal has made publicly available, which is precisely the material from which sexualised deepfakes are most often assembled. More fundamentally, its substantive obligations are not yet in force. Only the first phase of commencement, covering the definitions and the constitution of the Data Protection Board, took effect on 13 November 2025 with the notification of the rules made under the Act; the consent and data principal rights provisions in sections 3 to 17 are scheduled to commence in 2027.[37] A statute whose operative duties have not yet begun cannot be the answer to a harm occurring now.

C. Personality rights as a judge-made substitute

The statutory gap is thrown into relief by the wholly judge-made character of personality rights protection in India, a doctrine the Delhi and Bombay High Courts have developed over more than twenty years. In *ICC Development (International) Ltd. v. Arvee Enterprises* the Delhi High Court held that the right of publicity has evolved from the right of privacy and can inhere only

[36] *Id.* rr. 3(1)(d), 3(2)(b).

[37] The Digital Personal Data Protection Act, *supra* note 5, s. 1(2) and s. 3(c)(ii); Digital Personal Data Protection Rules, 2025 (India) (notified Nov. 13, 2025, with phased commencement).

 [ISSN 2581-5369]

in an individual, or in the indicia of an individual's personality such as name, personality trait, signature and voice, and not in a corporate or other non-living entity.[38]

The right was developed in *D.M. Entertainment (P) Ltd. v. Baby Gift House*, where the same court identified the right of publicity with an individual's autonomy to permit or refuse the commercial exploitation of his or her likeness, describing it as a quasi-property right and recasting it as a matter of dignity as much as of market control.[39] The contours of celebrity status were then defined in *Titan Industries Ltd. v. Ramkumar Jewellers*, in which the court set out a two-part test of validity and identifiability and held that infringement requires no proof of falsity, confusion or deception where the celebrity is identifiable.[40] That the whole body of Indian personality rights law rests on this line of common law precedent, rather than on the Information Technology Act or any other statute, confirms that a court confronting an AI-generated deepfake today is not applying a settled statutory scheme but extending a judge-made doctrine to a technology its original architects could not have anticipated.

IV. LESSONS FROM COMPARATIVE REFORM

A survey of international approaches to AI-generated content shows convergence on a small set of principles, chiefly transparency, accountability and stronger enforcement, alongside frameworks that remain fragmented and in many instances inadequate to the range of harms synthetic media produces. The European Union has taken the most systemic approach. The General Data Protection Regulation contains nothing specific to synthetic media and applies only through its general principles on lawfulness, special categories of data, rectification and erasure. The specific obligation lies in Article 50 of the Artificial Intelligence Act, which requires providers of generative systems to mark outputs in a machine-readable format detectable as artificially generated or manipulated, and requires deployers of a system producing a deepfake to disclose that the content has been artificially generated or manipulated, subject to exceptions for law enforcement and for evidently artistic, satirical or fictional work.[41] Those transparency duties became applicable on 2 August 2026 and, unlike the high-risk obligations, were not deferred by the subsequent amending regulation.

The United States has taken a more conduct-oriented approach, with enforcement built around the creation or distribution of harmful synthetic content rather than around disclosure at the

[38] *ICC Development (International) Ltd. v. Arvee Enterprises*, (2003) 26 PTC 245 (Del.) (India).
[39] *D.M. Entertainment (P) Ltd. v. Baby Gift House*, CS(OS) No. 893 of 2002 (Del. H.C. Apr. 29, 2010) (India).
[40] *Titan Industries Ltd. v. Ramkumar Jewellers*, (2012) 50 PTC 486 (Del.) (India).
[41] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, art. 50, 2024 O.J. (L 1689) (EU); Regulation 2026/1744 (EU) (deferring the high-risk obligations without deferring art. 50).

 [ISSN 2581-5369]

point of generation. The federal bill that would have imposed general disclosure requirements, the DEEPFAKES Accountability Act, has been introduced three times, in 2019, 2021 and 2023, and died in committee on each occasion; a further measure directed at digital replicas remains at the stage of introduction.[42] What has been enacted is narrower and correspondingly more effective. The TAKE IT DOWN Act, signed into law on 19 May 2025, requires covered platforms to operate a notice and removal process and, on a valid request, to remove a non-consensual intimate visual depiction, including a digital forgery, within forty eight hours, with enforcement by the Federal Trade Commission from May 2026.[43] The states have moved faster still: lawmakers in twenty two states passed twenty nine laws on explicit deepfakes in 2024 alone, and more than two hundred bills on election-related deepfakes have been introduced across the states.[44]

The United Kingdom's Online Safety Act 2023 is frequently described as imposing statutory takedown deadlines. It does not. Section 10(3) requires a provider to operate proportionate systems and processes designed to take down illegal content swiftly once alerted to it, and to minimise the time for which priority illegal content is present.[45] The duty attaches to the design of the system rather than to the disposal of any individual complaint, and no fixed period appears anywhere in the illegal content regime. The Act's substantive contribution lies elsewhere, in the intimate image offences it inserted into the Sexual Offences Act 2003, to which a further offence of creating or requesting the creation of a purported intimate image was added in 2025.[46] Academic assessment of the Act's application to non-consensual intimate deepfakes has been critical, and the comparison with the American statute is instructive: the fixed clock is in the United States instrument, not the British one.[47]

Among other developed economies, China has gone furthest towards mandatory provenance. The Provisions on the Administration of Deep Synthesis Internet Information Services took effect on 10 January 2023, and the Measures for Labelling AI-Generated Synthetic Content,

---

[42] DEEP FAKES Accountability Act, H.R. 3230, 116th Cong. (2019); DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. (2021); DEEPFAKES Accountability Act, H.R. 5586, 118th Cong. (2023); NO FAKES Act of 2025, S. 1367, 119th Cong. (2025).

[43] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, Pub. L. No. 119-12 (May 19, 2025); FEDERAL TRADE COMMISSION, *Complying With the Take It Down Act* (May 2026), https://www.ftc.gov/business-guidance/resources/complying-take-it-down-act.

[44] MULTISTATE, *Nonconsensual Deepfake Laws*, https://www.multistate.ai/nonconsensual-deepfake-laws (last visited Aug. 19, 2026); PUBLIC CITIZEN, *Tracker: State Legislation on Deepfakes in Elections*, https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/ (last visited Aug. 19, 2026).

[45] Online Safety Act 2023, c. 50, s. 10(3) (UK).

[46] *Id.* s. 188, inserting ss. 66B to 66D into the Sexual Offences Act 2003 (UK); Data (Use and Access) Act 2025, s. 138 (UK).

[47] Beatriz Kira, *When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the UK Online Safety Act*, 54 COMPUTER LAW & SECURITY REVIEW 106024 (2024), https://doi.org/10.1016/j.clsr.2024.106024.

together with the accompanying mandatory national standard, took effect on 1 September 2025. They require both an explicit label visible to the user and an implicit label carried in the file's metadata, and they oblige distribution platforms to detect and reinforce that labelling.[48] Taken together these efforts point to a common problem and a common remedy: digital trust, privacy and informed consent in an evolving AI environment can be protected only by regulatory intervention coupled with enforcement machinery that actually works.

V. Recommendations for reform in India

The case for targeted anti-deepfake legislation is straightforward. The offences on the statute book were not framed for harms generated by artificial intelligence, and the law must keep pace with the society and the technology that produce them. The European and American models are usefully read together. The European transparency approach is preventive, reducing the risk of harm before it occurs, while the American approach is remedial and permits the rapid identification of offenders, and the labelling of AI-generated content assists both by making the origin of synthetic material traceable. India has now adopted the transparency limb in subordinate legislation. What it has not done is put it on a statutory footing or attach a remedy to it.

The most intractable difficulty is that synthetic content propagates faster than it can be removed. Well drafted remedies are often less effective in execution than on paper. Once manipulated images, video or audio are released they spread quickly, and complete removal is extremely difficult and sometimes impossible. Reactive moderation systems that depend on complaints and on victim-driven reporting are correspondingly weak, because complaints are not always made and a victim may not know that her image has been manipulated at all.

Indian courts have addressed this through progressively firmer intermediary-directed relief. In *Ankur Warikoo v. John Doe*, decided by the Delhi High Court on 26 May 2025, deepfake videos had shown the plaintiff giving investment advice he had never given. The court directed the platform operator to remove the specifically identified pages, profiles and videos within thirty six hours, and gave the plaintiffs liberty to require the removal of future deepfakes within the same period, subject to liberty to return to the court if the platform raised any doubt.[49] The obligation was placed on the intermediary rather than on the infringing users, and the forward

[48] Measures for Labelling AI-Generated Synthetic Content (promulgated by the Cyberspace Administration of China, Mar. 14, 2025, effective Sept. 1, 2025) (China), read with mandatory national standard GB 45438-2025; Provisions on the Administration of Deep Synthesis Internet Information Services (promulgated Nov. 25, 2022, effective Jan. 10, 2023) (China).

[49] *Ankur Warikoo v. John Doe*, 2025 SCC OnLine Del 3727, CS(COMM) 514/2025 (Del. H.C. May 26, 2025) (India).

 [ISSN 2581-5369]

looking limb was deliberately not made unconditional. The Amendment Rules of 2026 have since gone further than the order did, cutting the corresponding administrative clock to two hours for non-consensual intimate imagery. That makes the case for statutory codification stronger rather than weaker. A timeline that exists only in delegated legislation can be relaxed as easily as it was imposed, and it gives the person depicted no enforceable right of her own. India should place explicit removal timelines for verified synthetic content in the statute book, so as to compress the window during which such content remains available and to protect privacy, dignity and consent in the digital sphere more effectively.

A further obstacle to enforcement is limited public understanding of the harm, which bears directly on a victim's willingness to report and to seek redress. Sustained public education can reduce that obstacle by making clear who is responsible, how the technology works and how an individual can tell whether she has been targeted. Such work would also reduce the social stigma that discourages reporting, particularly where the content is sexualised. The European Union pairs its regulatory instruments with media literacy obligations and programmes rather than with campaigns of its own, and the European Parliament's own research service has recommended precisely this combination in relation to deepfakes.[50] India would benefit similarly, both in rebuilding public confidence in regulatory institutions and in equipping younger users to recognise and respond to these harms. Wider public understanding would also strengthen detection, as the tools and the underlying mechanisms of deepfake creation become better known.

Deepfake abuse is, at its core, a violation of digital consent. Research on perpetrator and victim perspectives shows that those who create sexualised deepfakes commonly obtain their source material, photographs and video, from social media profiles, video calls and other ordinary online interaction, without the knowledge or permission of the person depicted.[51] A profile photograph that its subject has chosen to make public can be reworked into a sexualised image and then deployed by an acquaintance or a stranger to damage her reputation. Simple presence online thus creates an exposure to harassment that current legislation does little to mitigate. That is a direct infringement of digital consent and an argument for a consent-centred regulatory approach.

[50] M. van Huijstee et al., *Tackling Deepfakes in European Policy*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE, PE 690.039 (2021).

[51] Asher Flynn, Anastasia Powell, Asia Eaton & Adrian J. Scott, *Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery*, JOURNAL OF INTERPERSONAL VIOLENCE (advance online publication, Sept. 9, 2025), art. no. 08862605251368834, https://doi.org/10.1177/08862605251368834.

 [ISSN 2581-5369]

The Bombay High Court's order of 29 September 2025 in *Asha Bhosle v. Mayk Inc.* supports that framing. The court took the view that making artificial intelligence tools available to convert any voice into that of a celebrity, without permission, would itself violate that person's personality rights, and it restrained the use of the plaintiff's name, voice, vocal style and technique, image, likeness, signature and persona while ordering the disclosure of subscriber and seller data by the platforms before it.[52] The wrong lay in the taking of the voice, not in any deceptiveness or inaccuracy in what was produced. Sexualised deepfakes are, on the same analysis, not merely a technological problem but a consent harm, in which a person's likeness is used without agreement and in which victims face serious barriers to recognising the harm, obtaining prompt support and securing an effective remedy. That points to a dedicated digital consent regime and to a genuinely victim-centred regulatory response.

VI. Conclusion

Artificial intelligence promises efficiency, but its capacity to produce synthetic media poses a growing threat to individual dignity and to public trust. The social harms examined in this paper range across sexualised abuse, political manipulation, the liar's dividend as it affects journalism, and the cross-border enforcement difficulties that high-impact synthetic media fraud creates.

The Indian framework has not kept step. The Information Technology Act 2000 defines no deepfake-related offence, and the Digital Personal Data Protection Act 2023, although it will contribute to the privacy framework once its substantive provisions commence, contains no provision on synthetic identities or deceptive AI and excludes publicly available personal data from its scope altogether. The Amendment Rules of 2026 have closed part of the gap by defining synthetically generated information and imposing labelling and provenance duties, but they do so in delegated legislation that binds intermediaries alone, and they leave the person whose likeness has been taken without a remedy of her own. Neither statute deals adequately with the anonymity that decentralised networks afford, or with cross-border cybercrime.

India should therefore adopt a proactive rather than a reactive stance towards digital sovereignty, pairing continued technological development with legislation built on an adaptive and future-oriented framework capable of evolving with the technology. A combination of the American and European approaches offers a workable template, joining the conduct-based features of American regulation to the systemic transparency obligations of the Artificial Intelligence Act. The United Kingdom's Online Safety Act contributes a model of reporting and

[52] *Asha Bhosle v. Mayk Inc.*, Com. IP Suit (L) No. 30262 of 2025 (Bom. H.C. Sept. 29, 2025) (India).

 [ISSN 2581-5369]

complaint machinery, though not, as is often supposed, of statutory takedown deadlines, and any Indian framework must be enforceable if the public is to trust it.

VII. THE WAY FORWARD

There should be a statutory right to one's digital likeness, framed as a standalone civil cause of action. At present the protection described above exists only in judicial precedent obtained by those who can afford it. A complainant of ordinary means cannot realistically bear the cost of a commercial suit in a High Court, and delay is itself a denial of the remedy. Parliament should codify a statutory tort of non-consensual digital likeness appropriation, available through a low-cost, time-bound summary proceeding before a district-level forum such as the District Consumer Disputes Redressal Commission. A dedicated cyber tribunal would serve the same end, displacing the present dependence on High Court injunctions and offering both speedy removal of synthetic content and affordable litigation.

Where a complainant files a takedown request, the platform to which it is addressed should bear the burden of showing that the content is authentic or consented to, rather than the complainant bearing the burden of showing that it is not. The Amendment Rules of 2026 have shortened the administrative clock considerably, but they have not reversed the burden, and the burden is the more important of the two. It is the virality of the material that causes the harm, not the eventual legal victory. Alongside this, developers of AI models and of deepfake-generating tools operating in India should be required to apply invisible cryptographic watermarks at the moment of generation, enforced through licensing conditions on the tool providers. Because developers are far fewer than users, control exercised at the point of generation propagates automatically to the whole user population, and it would give the labelling duty already imposed on intermediaries something reliable to work with.

There should also be a dedicated synthetic media unit within the Indian Cyber Crime Coordination Centre, empowered to issue emergency takedown directions without a court order. The purpose is to spare a member of the public the necessity of drafting a writ petition each time material has to be removed, which at present converts a remedy into a delay. The unit's powers should be exercised administratively, its directions should be binding, and they should be subject to defined time limits and to a route of appeal.

Finally, India is not a party to the Budapest Convention on Cybercrime and has never signed it, the objections most consistently advanced being that India did not participate in its drafting and that Article 32(b), which permits transborder access to stored computer data without the consent of the state in which the data is located, is difficult to reconcile with sovereignty. India is

 [ISSN 2581-5369]

likewise not among the signatories to the United Nations Convention against Cybercrime adopted in December 2024.[53] Whatever the merits of accession, the practical consequence is that cross-border evidence collection in deepfake cases depends on bilateral cooperation. India should therefore pursue bilateral and plurilateral mutual legal assistance arrangements with the jurisdictions that matter most, among them the United States, Singapore and Ireland, where the principal platform entities are established. That would establish an initial capacity to address cross-border jurisdictional problems, directed at the platforms that carry most of the traffic, without the exposure that accession to a large multilateral treaty would entail.

*****

[53] Convention on Cybercrime, opened for signature Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004); United Nations Convention Against Cybercrime, G.A. Res. 79/243 (Dec. 24, 2024).

 [ISSN 2581-5369]